Human Risk Review 2021

Eine Analyse der europäischen Cyber-Bedrohungslage

SoSafe
Cyber Security Awareness

Editorial

Warum ist genau jetzt ein guter Zeitpunkt, sich den Faktor Mensch in der IT-Sicherheit (noch) genauer anzuschauen?

Das vergangene Jahr war – nicht zuletzt durch die COVID-19-Pandemie – ein Jahr der Herausforderungen für uns alle. Cyberkriminelle haben diese Situation schamlos ausgenutzt und uns angegriffen, als wir am verletzlichsten waren. Schon kurz nach Ausbruch des Infektionsgeschehens konnten wir Phishing-Kampagnen beobachten, die sich die angespannte Lage zunutze machten. Es wurden Angriffe konzipiert, die mit den Emotionen der Menschen spielten und letztlich ganze Infrastrukturen lahmlegten. Schnell war klar: Die Angreifenden nutzen diese Krise ohne Skrupel für Social-Hacking-Attacken aus.

Die ENISA spricht von einem Anstieg von Phishing-Mails um mehr als 600 %. Phishing-Webseiten sind laut Google auf einem Rekordhoch.

Diverse Studien belegen diese Beobachtungen mittlerweile ganz eindeutig – mit teils erschreckenden Zahlen. Die Agentur der Europäischen Union für Cybersicherheit (ENISA) spricht von einem Anstieg von Phishing-Mails um mehr als 600 %. Phishing-Webseiten sind laut Google auf einem Rekordhoch. Und Interpol warnt in einem Bericht eindringlich vor den Cybergefahren, die uns auch nach der Krise in einer veränderten Arbeitswelt begleiten werden. Die dabei entstehenden Schäden nehmen ebenfalls zu: Die jährliche Summe hat sich laut Bitkom seit 2017 bereits mehr als verdoppelt.

Was aber macht die aktuelle Gefahrenlage so akut und gerade menschenbasierte Angriffe so erfolgreich? Unsere Auswertungen lassen vor allem zwei Faktoren vermuten:

Emotionale Verunsicherung

Die Pandemie hatte und hat einen nachhaltigen Einfluss auf die Psyche der Menschen und ganze Nationen an ihre Belastungsgrenze gebracht. Diese angespannte Lage spielt Cyberkriminellen in die Karten – sie können uns über Social Engineering und neue psychologische Taktiken wie das Bedürfnis nach Schutz noch gezielter austricksen.

New Work und Homeoffice-Modelle

Zum Schutz unserer Mitmenschen arbeiten wir nun vermehrt von zu Hause – aber auch nach Abklingen der Krise wird Remote Work eher Regel als Ausnahme sein. Die neuen Arbeitsweisen und Tools sind für viele Mitarbeitende allerdings ungewohnt und bieten Cyberkriminellen neue Angriffspunkte. Der Umgang mit sensiblen Informationen im Homeoffice muss von einer großen Gruppe an Nutzenden erst noch erlernt werden. Gleichzeitig entfällt beispielsweise der Flurfunk im Büro, der vor allem dann wertvoll ist, wenn es um das Erkennen von Angriffen geht.

Der Mensch und seine Emotionen stehen also ganz besonders im Fadenkreuz, und Social-Engineering-Hacks gewinnen weiter an Bedeutung. Dabei nimmt nicht nur das Angriffsniveau zu, auch die Taktiken verschärfen sich: Methoden wie „Double Extortion“ werden immer häufiger eingesetzt und vermindern den Effekt von Maßnahmen zum Schutz oder zur Schadensbehebung, etwa von Back-ups.

In diesem Report ordnen wir daher das wachsende Human Risk ein, blicken zurück auf 2020 und nach vorn auf das neue Jahr: Mit welchen psychologischen Tricks und Maschen sind wir besonders angreifbar? Was sind die größten Gefahren für die IT-Sicherheit? Und wie können Organisationen ihr Risiko, einem Cyberangriff zum Opfer zu fallen, in Zukunft minimieren?

Unsere Auswertung stützt sich auf vier Datenquellen: über 1,4 Millionen Datenpunkte aus unserer SoSafe Awareness-Plattform, eine gezielte Erhebung zur Phishing-Awareness mit mehr als 5.000 Teilnehmenden, Analysen aus der AV-TEST Threat Intelligence Plattform und eine Befragung unter mehr als 100 IT-Sicherheitsexpertinnen und -experten.

Wenn die Ergebnisse eines zeigen, dann, dass Cyber Security uns alle angeht. Nie war es wichtiger, sich selbst und andere vor den Gefahren aus dem Netz zu schützen. Was für unsere Gesundheit gilt, gilt auch für die IT-Sicherheit: Prävention ist besser als Schadensbehebung.

Dr. Niklas Hellemann
Managing Director, SoSafe GmbH

Inhaltsverzeichnis

Executive Summary 4

Gefahrenlage 2020: Cyberangriffe sind das größte Betriebsrisiko 5

Phishing, Ransomware, Trojaner: Wie sich das Angriffspotenzial weiter verschärft 6

Infobox: Cybercrime im Gesundheitswesen – ein Exkurs 9

Analyse der europäischen Cyber Threat Landscape 2020
Datenbasis und Methodik 11

Infobox: Datenabkommen Privacy Shield revidiert – Nur EU-Dienstleister bieten Rechtssicherheit 13

So schätzen Sicherheitsexpertinnen und -experten das Angriffspotenzial ein 14

Infobox: Prävention im Bereich IT-Sicherheit ist Chefsache 17

Interview: Warum Airbags nicht vor Unfällen schützen – Die Wichtigkeit des Faktors Mensch in der IT-Sicherheit 18

Malware: Der dramatische Anstieg im Überblick 21

Infobox: Schutzfaktor Flurfunk – die Organisationsstruktur als Einflussfaktor? 24

Psychologische und technische Vektoren – die Risikofaktoren im Überblick 25

Top-10-Betreffzeilen 2020 29

Interview: Präventive und reaktive Cyber Security Awareness – IT Sicherheit als Gemeinschaftsprojekt 35

Das Klickverhalten im Detail: Welchen Einfluss haben Demografie, Branche und Uhrzeit? 37

Interview: Herausforderung Homeoffice – IT-Sicherheit in Zeiten zunehmender Digitalisierung 41

Social-Engineering-Trends 2021: Cyberkriminelle rüsten weiter hoch 43

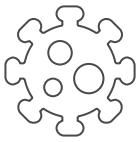
Fazit & Empfehlungen: Wie minimieren Organisationen ihr Human Risk? 46

Über SoSafe 47

Executive Summary

Homeoffice macht anfälliger für Cyberangriffe

75 % der befragten IT-Sicherheitsexpertinnen und -experten gehen davon aus, dass das neue Homeoffice-Setting erfolgreiche Cyberangriffe wahrscheinlicher macht. Dies zeigt sich auch in den Klickdaten: Unsere Analysen ergeben, dass die Klickrate auf Phishing-Mails in dezentralen Organisationen (beziehungsweise bei Remote Work) signifikant höher ist als in zentral aufgestellten Organisationen (beziehungsweise bei Präsenzarbeit). Dementsprechend plant die Mehrheit der befragten Entscheiderinnen und Entscheider auch, mit dem Wechsel ins Homeoffice die Maßnahmen zur Sensibilisierung der Mitarbeitenden zu erhöhen oder zumindest beizubehalten.



Die Coronakrise als Fest für Cyberkriminelle

Cyberkriminelle nutzen Krisen – wie aktuell durch das Coronavirus – und gesellschaftliche Instabilität für ihre Zwecke aus und fahren ihr Angriffsvolumen in solchen Zeiten weiter hoch. Die Auswertungen zeigen einen rapiden Anstieg an Ransomware-Typen in diesem Jahr, insbesondere während des ersten Lockdowns im März 2020. Das gleiche gilt für deren Erfolgswahrscheinlichkeit: In der Phase des ersten Lockdowns war die Klickrate bei Phishing-Mails stark erhöht.

Erfolgreiche Social-Engineering-Maschen durch Coronabezug

Cyberkriminelle haben bereits in den ersten Wochen der Pandemie Corona-spezifische Inhalte in Phishing-Kampagnen einfließen lassen. Unsere Analysen zeigen nachweislich, dass dies auch zu einer erhöhten Erfolgswahrscheinlichkeit führt. Corona-Phishing-Mails oder E-Mails, die die Einführung von Remote-Tools adressieren, führen unser Ranking der erfolgreichsten Phishing-Mails an. Während die durchschnittliche Klickrate bei 29 % liegt, zeigen E-Mails mit dem Wort „Corona“ im Betreff Klickraten bis zu 78,8 %.

Trojaner weiter auf dem Vormarsch

Trojaner sind weiterhin der gefährlichste Malware-Typ – sie machen 55 % der bekannten Schadsoftware aus. Auch die Gesamtmenge an neuer Malware erreichte 2020 mit 750 Millionen eine noch nie da gewesene Dimension.

Angriffe ohne Skrupel – KRITIS im Visier

Angriffe auf Organisationen der kritischen Infrastruktur (KRITIS) haben im vergangenen Jahr laut Bundesregierung um 50 % zugenommen. Dabei ist die Erfolgsrate simulierter Phishing-Angriffe – und damit auch das Risiko, einem Cyberangriff zum Opfer zu fallen – zum Beispiel in Krankenhäusern im Vergleich zum Durchschnitt um 30 % erhöht. Besonders skrupellos: Auch die Herstellungs- und Lieferkette für die Corona-Impfstoffe steht oftmals im Fokus der Attacken.

Digital Natives klicken am häufigsten auf Phishing-Mails

In einer separaten Studie mit 5.000 Teilnehmenden analysierten wir das Klickverhalten von Bürgerinnen und Bürgern – auch unter Berücksichtigung demografischer Variablen. Der Mythos des „Digital Natives“ suggeriert, dass jüngere Nutzende sicherer im Umgang mit IT sind. Die Ergebnisse zeigen jedoch, dass 18- bis 29-Jährige mit einer Klickrate von 38 % häufiger auf Phishing-Mails klicken als alle anderen Altersgruppen mit durchschnittlich nur 25 %.

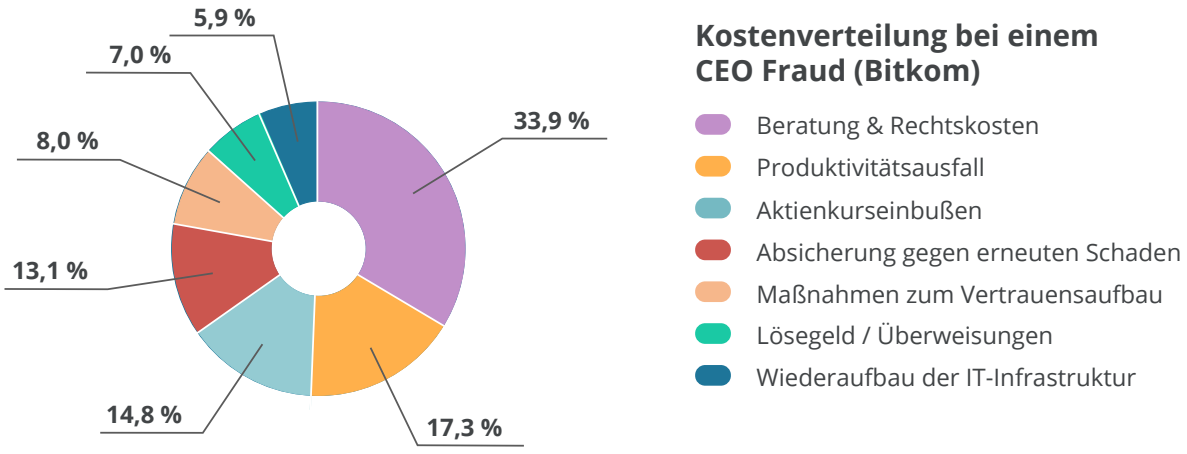
Gefahrenlage 2020: Cyberangriffe sind das größte Betriebsrisiko

2020 hat für viele unerwartete Wendungen gesorgt – auch und vor allem im Bereich IT-Sicherheit. Eines hat sich aber bei alledem nicht geändert: Cyberkriminalität bleibt weiterhin eine ernst zu nehmende Gefahr für Organisationen verschiedenster Größen und Branchen. So rangiert Cybercrime im jährlichen Ranking des World Economic Forums auf Platz drei der größten Bedrohungen für die weltweite Wirtschaft. Die Hälfte aller Unternehmen befürchtet demnach Cyberattacken und Datenbetrug, etwa durch veränderte Arbeitsmuster wie Homeoffice-Modelle.[1]

Die Relevanz bestätigen auch andere offizielle Bewertungen der Cyber-Gefahrenlage: In einem Studienbericht zum Wirtschaftsschutz berichtet der Bitkom[2] von jährlichen Schäden über 100 Milliarden Euro – allein in Deutschland. Das Sicherheitsunternehmen McAfee[3] schätzt den globalen Schaden auf mehr als 1 Billion US-Dollar.

Die Kosten eines Cybervorfalls belaufen sich nicht selten auf Millionenbeträge

Für Organisationen heißt das konkret: Erfolgreiche Angriffe werden immer wahrscheinlicher – und sie können teuer werden. In einem vom Bitkom berechneten fiktiven Fallbeispiel eines Cybervorfalls in einem mittleren deutschen Produktionsunternehmen wird die mögliche Schadenshöhe bei einem CEO Fraud auf mehr als 6,6 Millionen Euro geschätzt.[4] Während ein etwaiger über Social Engineering erschlichener Überweisungsbetrag mit nur 7,5 % minimal ins Gewicht fällt, sind vor allem die Kosten zur Behebung der Schäden und zum Wiederaufbau von Vertrauen und Image nach einer Attacke laut Bitkom hoch. Zu beachten ist jedoch, dass auch die Höhe von direkten Lösegeldforderungen bei anderweitigen Cybervorfällen gestiegen ist (siehe auch S. 8). So „rühmte“ sich erst im Sommer 2020 das amerikanische Reiseunternehmen CWT damit, die Erpresser von ursprünglich 10 Millionen US-Dollar auf 4,5 Millionen US-Dollar heruntergehandelt zu haben.[5]

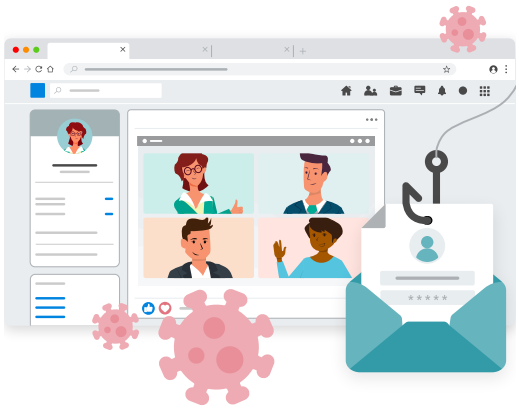


[1] World Economic Forum (2020). COVID-19 has disrupted cybersecurity, too - here's how businesses can decrease their risk.
[2] Bitkom (2020). Spionage, Sabotage und Datendiebstahl - Wirtschaftsschutz in der vernetzten Welt.
[3] McAfee (2020). New McAfee Report Estimates Global Cybercrime Losses to Exceed $1 Trillion.
[4] Bitkom (2016). Kosten eines Cyber-Schadenfalles. Leitfaden.
[5] Reuters (2020). 'Payment sent' - travel giant CWT pays $4.5 million ransom to cyber criminals.

Phishing, Ransomware, Trojaner: Wie sich das Angriffs-potenzial weiter verschärft

Erstmals scheinen auch die Organisationen selbst dieses enorme Risikopotenzial erkannt zu haben: Im Allianz Risk Barometer[6] geben Unternehmen weltweit Cyberangriffe als größtes Risiko für ihr Geschäft an. Einer der Gründe dafür ist sicherlich auch, dass Angriffstaktiken laufend weiterentwickelt werden und es Organisationen so erschweren, sowohl effektive Schutzmaßnahmen zu treffen als auch im Ernstfall zu reagieren. Doch welche neuen Taktiken standen 2020 im Vordergrund? Welche Angriffe waren besonders erfolgreich? Welche Trends lassen sich beobachten?

Auf Basis der Einschätzungen unserer Expertinnen und Experten, Kundinnen und Kunden und Partnerorganisationen geben wir im Folgenden einen Überblick über die komplexen Methoden der Cyberkriminellen und Entwicklungen, die im letzten Jahr Organisationen weltweit in Atem gehalten haben.

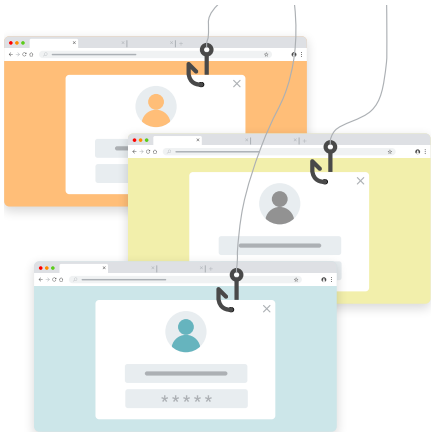


Die Krise befeuert Social Engineering

Wie kaum ein anderes Jahr bot sich 2020 für Cyberkriminelle an, um neue Spam- und Phishing-Kampagnen in Umlauf zu bringen. Gesellschaftlich relevante und medienwirksame Debatten wurden ohne Zögern für kriminelle Zwecke missbraucht und die emotional sensiblen Themen ausgenutzt. Interpol berichtete in seinem COVID-19 Cybercrime Analysis Report[7] von einem enormen Anstieg an Angriffen, die sich die Krise zunutze machten.

Laut der ENISA[8] waren darunter sechsmal so viele Phishing-Attacken wie noch zuvor. Daneben sorgten auch die #blacklivesmatter Bewegung und die US-Wahlen für eine Flut an perfiden (Spear-) Phishing-Attacken, die ihre Opfer emotional manipulierten.

[6] Allianz (2021). Allianz Risiko Barometer 2021: Covid-19-Trio an der Spitze der Unternehmensrisiken
[7] Interpol (2020). Interpol report shows alarming rate of cyberattacks during COVID-19.
[8] Europäische Agentur für Cybersicherheit (ENISA) (2020). Understanding and dealing with phishing during the covid-19 pandemic.



Phishing-Webseiten weiter im Aufwärtstrend

Ein neuer Negativrekord: Google[9] entdeckte 2020 mehr als 2 Millionen Phishing-Webseiten – ein Anstieg um etwa 20 % im Vergleich zum Vorjahr. Immer mehr dieser Seiten nutzen dabei außerdem SSL-Zertifikate. Ein einfacher Blick auf die URL beziehungsweise das Protokoll reicht also nicht mehr aus, um eine Seite als gefährlich zu identifizieren. Zurückzuführen sind die hohen Zahlen wohl nicht zuletzt auf die COVID-19-Pandemie – im ersten Halbjahr registrierte Google knapp 50.000 neue Phishing-Seiten pro Woche und damit weitaus mehr als noch kurz zuvor.

Ein nur kurzlebiger Trend ist dies allerdings nicht: Seit 2015 steigen die Zahlen jedes Jahr um knapp 13 %. Die Coronakrise hat die allgemeine Entwicklung also lediglich beschleunigt.

Kritische Infrastrukturen im Fokus

Auch in der Krise schreckten opportunistische Cyberkriminelle nicht vor Angriffen auf den KRITIS-Bereich zurück: Einrichtungen wie Krankenhäuser wurden angegriffen, Infrastrukturen lahmgelegt und sensible Daten ohne jegliche Moral zur Erpressung von Lösegeldern gestohlen.

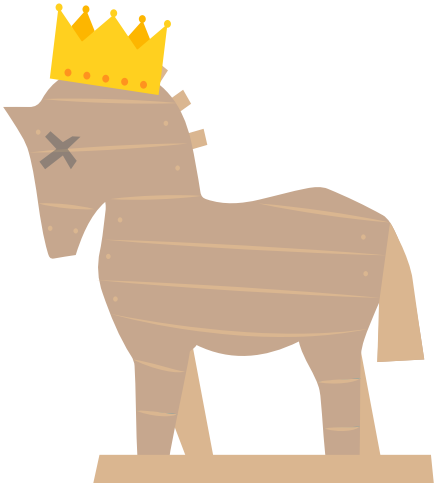
Nach einer Cyberattacke auf die finnische Psychotherapieklinik Vastaamo wurden sogar die Patientinnen und Patienten selbst mit dem Inhalt ihrer vertraulichen Krankenakten erpresst. Interpol berichtete Anfang Dezember außerdem von vermehrten direkten und indirekten Angriffen auf die Impfstoffketten, bei denen nicht nur Regierungen, sondern auch verunsicherte Einzelpersonen ins Fadenkreuz gerieten.[10] Die gesellschaftliche Schlüsselfunktion macht das Geschäft im KRITIS-Bereich für die Kriminellen besonders lukrativ (siehe Infobox S. 9).

[9] Forbes (2020). Google Registers Record Two Million Phishing Websites in 2020.
[10] Interpol (2020). Interpol warns of organized crime threat to COVID-19 vaccines.

Cyberkriminelle auf Großwildjagd

Schon in den letzten Jahren konnte man nur staunen über die enormen Lösegeldforderungen, die Cyberkriminelle nach Ransomware-Attacken stellten. 2020 gingen sie in die Vollen, attackierten auch die größten Konzerne und schraubten die Lösegelder weiter in die Höhe. Insgesamt kam es zu einer Zunahme von über 40 % bei erfolgreichen Ransomware-Angriffen weltweit.[11] Der Navigationsspezialist Garmin zahlte im Juli vermeintlich circa 10 Millionen US-Dollar an die Angreifenden. Im englischsprachigen Raum hat sich für die Taktik der Cyberkriminellen schnell der Begriff „Big Game Hunting", auf Deutsch „Großwildjagd", etabliert.

Die Zahlen sprechen für sich: Laut Accenture[12] stieg die durchschnittliche Lösegeldzahlung von Q1 zu Q2 2020 nochmals um 60 % an. Aber auch kleine und mittlere Unternehmen stehen weiterhin im Fokus der Ransomware-Attacken: Vier von fünf mittleren und jedes fünfte kleine Unternehmen wurde gezielt angegriffen.[13]



Trojaner als bewährte Allzweckwaffe

Im Januar 2021 gelang es dem Bundeskriminalamt (BKA) in Zusammenarbeit mit internationalen Behörden sowie Europol und Eurojust, den „König der Malware"[14] Emotet zu zerschlagen[15]. Im vergangenen Jahr sorgte er nach einer kurzen Unterbrechung im Sommer aber noch für Aufruhr unter IT-Spezialistinnen und -Spezialisten. Das Gefährliche: Mit ihrem oftmals polymorphen Design entgehen Trojaner wie Emotet oder Egregor immer wieder technischen Filtern.

In neueren Versionen setzte Emotet etwa auf Thread Hijacking – stahl also tatsächlich versendete Mail-Konversationen, um diese mit schädlichen Inhalten fortzuführen. Die Daten von AV-TEST (siehe S. 21) belegen, dass Trojaner auch 2020 die am häufigsten genutzte Malware waren und damit im Fokus von Sicherheitsmaßnahmen stehen sollten. Mit immer wieder neuen Malware-Typen halten Cyberkriminelle IT-Verantwortliche auch weiterhin auf Trab – die Zerschlagung der Emotet-Infrastruktur ist wohl nur ein vorübergehender Grund zum Aufatmen.

[11] Heimdal (2020). This Year in Ransomware Payouts.
[12] Accenture (2020). Cyber Threatscape Report.
[13] Heimdal (2020). This Year in Ransomware Payouts.
[14] Golem (2019). „Emotet ist der König der Schadsoftware".
[15] Bundeskriminalamt (2021). Infrastruktur der Emotet-Schadsoftware zerschlagen.

Infobox

Cybercrime im Gesundheitswesen – ein Exkurs

Kritische Infrastrukturen (KRITIS), darunter Wasser- und Energieversorger, die Lebensmittelindustrie oder das Gesundheitswesen, gelangen immer häufiger ins Fadenkreuz von Cyberkriminellen. Durch eine zunehmende Vernetzung und Digitalisierung sind sie gleichzeitig aber auch immer angreifbarer. Bei einem Ausfall der KRITIS drohen gravierende Konsequenzen für das öffentliche Leben. Das macht sie zum perfekten Zielobjekt für Attacken auf die IT und zur Forderung von enormen Lösegeldern.

Insbesondere Krankenhäuser sind aktuell wegen ihrer gesellschaftlichen Relevanz und spezifischen Arbeitsabläufe interessante Ziele für Cyberkriminelle. Kein Bereich der kritischen Infrastruktur hat im letzten Jahr mehr IT-Sicherheitsvorfälle gemeldet als der Gesundheitssektor. Die Zahl an Cyberangriffen auf die Einrichtungen hat sich laut Bundesregierung in Deutschland von 2019 auf 2020 verdoppelt.[16] Grund für das hohe Angriffspotenzial sind neben veralteten Systemen auch komplexe Arbeitsabläufe (etwa Schichtbetrieb) und nicht zuletzt die enorme Belastung durch die COVID-19-Pandemie. So ist letztlich die Erfolgsrate bei simulierten Phishing-Angriffen um 30 % höher als im Durchschnitt.[17]

[16] Frankfurter Allgemeine (2020). Hacker greifen Kliniken an.
[17] SoSafe Awareness-Plattform.

Fallbeispiel: Ransomware setzt Notfallbetrieb in Düsseldorfer Uniklinik aus

Im September 2020 wird die Ransomware-Attacke auf das Universitätsklinikum in Düsseldorf bekannt. Der in das Uniklinikum eingeschleuste Erpressungstrojaner verschlüsselt 30 Server und legt nicht nur die IT-Systeme, sondern auch den Notfallbetrieb für 13 Tage lahm. Es dauert trotz schneller Entschlüsselung knapp zwei Wochen, bis alle Systeme wieder laufen. Besonders dramatisch: Eine dringend benötigte Notfallversorgung kann nicht angeboten werden. Die Fahrt in ein deutlich weiter entferntes Krankenhaus in Wuppertal kostet einer Patientin das Leben. Inzwischen hat auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) den Fall analysiert und geht davon aus, dass er mit entsprechenden präventiven Maßnahmen hätte vermieden werden können.[18]

Das Krankenhauszukunftsgesetz

Auch der Gesetzgeber hat die Brisanz der zunehmenden Cyberangriffe auf Krankenhäuser mittlerweile erkannt und investiert in präventive Maßnahmen. Im Oktober 2020 wurde das Krankenhauszukunftsgesetz (KHZG)[19] beschlossen – ein milliardenschweres Förderpaket für Kliniken, das von Bund und Ländern gemeinsam ins Leben gerufen wurde.

Noch bis Ende des Jahres 2021 können Krankenhäuser ihren Anspruch auf Förderung mit einem umfassenden Antrag geltend machen. Gefördert wird neben dem Ausbau von modernen Notfallkapazitäten oder geschlossenen Medikationsprozessen auch eine bessere digitale Infrastruktur, zum Beispiel in Form von Maßnahmen zur IT-Sicherheit. Diese müssen laut den Richtlinien mindestens 15 % des Förderbetrags in Anspruch nehmen. In den Förderrichtlinien werden dabei explizit auch Cyber-Security-Awareness-Lösungen genannt.

Dort heißt es: „Förderfähige Vorhaben zur Verbesserung der IT- bzw. Cybersicherheit müssen: [...] die Steigerung und Aufrechterhaltung der Awareness gegenüber Informationssicherheits-Vorfällen bzw. der Bedeutung von IT-/Cybersicherheit (u.a. regelmäßige Risikoanalysen, Schulungsmaßnahmen, Informationskampagnen, Awareness-Messungen) [...] zum Ziel haben“ (vgl. Förderrichtlinie nach § 21 Abs. 2 KHSFV[20]). Auch SaaS-Lösungen sind laut KHZG förderfähig. Wichtig allerdings: Anbieter müssen vom Bundesamt für Soziale Sicherung zertifiziert und vor allem voll DSGVO-konform sein, d.h., es muss sich um europäische Anbieter handeln.

[18] rp-online (2021). Hackerattacke auf Uniklinik Düsseldorf wäre verhinderbar gewesen.
[19] Bundesministerium für Gesundheit (2020). Kabinett beschließt umfassendes Investitionsprogramm für Krankenhäuser.
[20] Bundesministerium für Soziale Sicherung (2020). Richtlinie zur Förderung von Vorhaben zur Digitalisierung der Prozesse und Strukturen im Verlauf eines Krankenhausaufenthaltes von Patientinnen und Patienten nach § 21 Absatz 2 KHSFV.

Analyse der europäischen Cyber Threat Landscape 2020: Datenbasis und Methodik

Auf Basis umfangreicher Datenquellen fasst dieser Report die Gefahrenlage 2020 zusammen und erörtert die Frage: „Wie hoch ist und war das Human Risk für Organisationen?“ Die Ergebnisse stützen sich dabei sowohl auf quantitative als auch auf qualitative Analysen und ermöglichen einen umfassenden Überblick über Status quo und aktuelle Entwicklungen der Cyber Threat Landscape mit besonderem Augenmerk auf den Faktor Mensch. Konkret sind vier Datensätze/Analysen in diesem Report enthalten:

Datensatz 1: Malware-Analyse aus der AV-TEST Threat Intelligence Plattform

Auswertungen der AV-TEST GmbH, einem führenden unabhängigen Forschungsinstitut für IT-Sicherheit, beleuchten die Bedrohungslage aus technischer Perspektive. Die Threat Intelligence Software von AV-TEST (AV-ATLAS[21]) analysiert und klassifiziert Malware vollautomatisiert.

3 Mio.

gescannte Dateien pro Tag

25

Virenscanner für vollautomatisierte Threat Intelligence

> 700 Mio.

Schadprogramme in der Datenbank erfasst

Die AV-TEST-Analysen erlauben es so, einen statistisch informierten Rückblick auf die technische Seite der Cyber Threat Landscape 2020 zu werfen. Welche Malware-Kategorien waren am häufigsten, und welche Rückschlüsse lassen sich auch aus der zeitlichen Entwicklung ziehen?

Datensatz 2: Reaktionsdaten aus der SoSafe Awareness-Plattform

Exklusive Reaktionsdaten aus der SoSafe Awareness-Plattform geben demgegenüber einen Einblick in die psychologische Seite der Angriffe und beantworten auch Fragen nach der Erfolgswahrscheinlichkeit verschiedener menschenbasierter Angriffe, beispielsweise Phishing.

1,4 Mio.

ausgewertete simulierte Phishing-Angriffe aus 2020

200

Kundenorganisationen in Reaktionsanalysen erfasst

Für die SoSafe Phishing-Simulation werden Millionen von Datenpunkten über die aktuelle Bedrohungslage sowie die Reaktionen von Mitarbeitenden im Falle eines vermeintlichen Angriffs gesammelt – Letzteres vollständig anonym (für die Bedeutung der Informationsverarbeitung im Rahmen der DSGVO und durch EU-Anbieter siehe Infobox S.13).

[21] AV-TEST - The Independent IT-Security Institute (2021). AV-ATLAS.

Neben technischen und psychologischen Faktoren, die den Erfolg von Phishing-Mails quantifizieren, enthalten die Analysen auch branchenspezifische Vergleiche und Einblicke in das Klickverhalten der Nutzenden, zum Beispiel im Hinblick auf Zeiten. Die Auswertungen lassen demnach nicht nur Schlussfolgerungen zu Cyber-Security-Schwachstellen in Organisationen zu, sondern ermöglichen es auch, auf Basis der Daten Ansätze für die Stärkung der IT-Sicherheit zu entwickeln.

Datensatz 3: Phishing-Simulation „Phish-Test“ zur Erhebung der allgemeinen Awareness

Als weitere Datenquelle dient eine jährlich von SoSafe und Botfrei.de durchgeführte Studie zur allgemeinen Phishing-Awareness der Bevölkerung. Über 5.000 User nahmen an der letzten Phishing-Simulation im Oktober 2020 teil. Alle Teilnehmenden erhielten nach der Registrierung innerhalb von einer Woche drei simulierte, aber realistisch wirkende Phishing-Mails, die es zu erkennen galt. Die Auswertung der Ergebnisse unter Berücksichtigung der demografischen Daten der Teilnehmenden ermöglichen tiefer gehende Rückschlüsse in Bezug auf deren Klickverhalten.

Datensatz 4: Befragung von IT-Sicherheitsexpertinnen und -experten

Schließlich werden die datengetriebenen Analysen in diesem Report durch eine repräsentative Befragung von mehr als 100 Expertinnen und Experten aus dem Cyber-Security-Bereich ergänzt. Die Antworten geben Aufschluss darüber, wie IT-Sicherheitsverantwortliche die von der COVID-19-Pandemie geprägte Gefahrenlage im letzten Jahr wahrgenommen haben. Sie geben außerdem einen Eindruck vom aktuellen Stand der Awareness-Bemühungen in Organisationen. In Interviews mit ausgewählten Expertinnen und Experten wird noch intensiver analysiert und evaluiert, welche Rolle der Faktor Mensch sowie Awareness-Maßnahmen in Zukunft spielen werden.

Infobox

Datenabkommen Privacy Shield revidiert – nur EU-Dienstleister bieten Rechtssicherheit

Im sogenannten Schrems-II-Urteil vom 16. Juli 2020 hat der Europäische Gerichtshof das „Privacy Shield"-Abkommen zwischen Europa und den USA für nichtig erklärt. Europas höchste Rechtsprechungsinstanz sagt damit eines deutlich aus: Das in der Datenschutzgrundverordnung geforderte Sicherheitsniveau zur Verarbeitung von Daten von EU-Bürgerinnen und -Bürgern kann in den USA aktuell nicht sichergestellt werden.

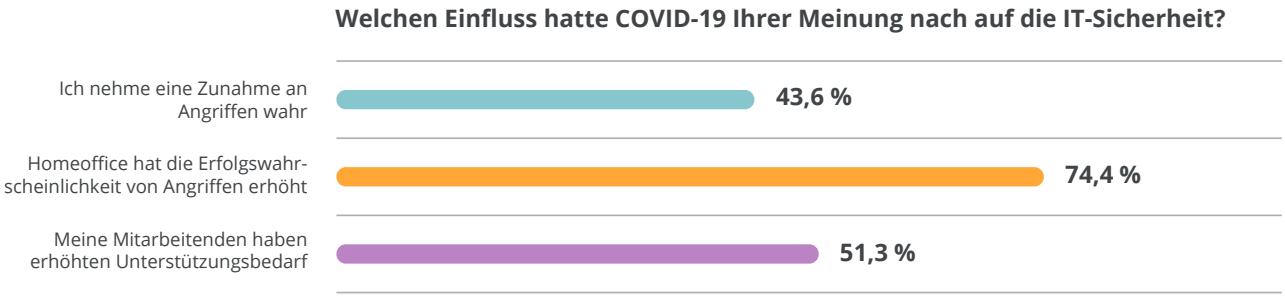
Für Organisationen kann diese Rechtsprechung weitreichende Folgen haben. Werden Dienste von Nicht-EU-Unternehmen in Anspruch genommen, begibt man sich in eine rechtliche Grauzone – insbesondere im Bereich der Schulung von Mitarbeitenden, während derer teils sensible Daten verarbeitet werden. Mitarbeiterinnen und Mitarbeiter können entsprechend gegen die Verarbeitung durch einen Nicht-EU-Anbieter Beschwerde bei den Aufsichtsbehörden einlegen. Im schlimmsten Fall droht so ein Bußgeld von bis zu 4 % des weltweiten Jahresumsatzes sowie rechtliche Auseinandersetzungen mit Mitarbeitenden. Für absolute Rechtssicherheit sorgt daher nur eine Datenverarbeitung auf EU-Servern durch ein europäisches Unternehmen.

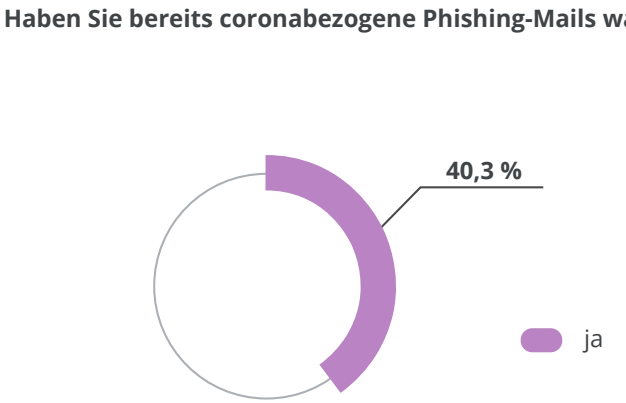
So schätzen Sicherheitsexpertinnen und -experten das Angriffspotenzial ein

Organisationen erkennen erhöhtes Angriffspotenzial

Unsere Befragung unter IT-Sicherheitsexpertinnen und -experten (Datensatz 4) bestätigt, dass sich Organisationen durchaus über den Anstieg von Cybergefahren bewusst sind und einen direkten Einfluss der Coronapandemie auf die IT-Sicherheit in ihrer Organisation erkennen.

Mehr als die Hälfte der Befragten geben an, dass die Mitarbeitenden in der Krise einen erhöhten Unterstützungsbedarf haben. Knapp 75 % gehen sogar davon aus, dass sich durch das vermehrte Arbeiten von zu Hause auch die Wahrscheinlichkeit von erfolgreichen Cyberangriffen erhöht. Immerhin vier von zehn Befragten sind bereits selbst Zeuge der verschärften Bedrohungslage geworden und konnten COVID-19-bezogene Phishing-Mails beobachten.

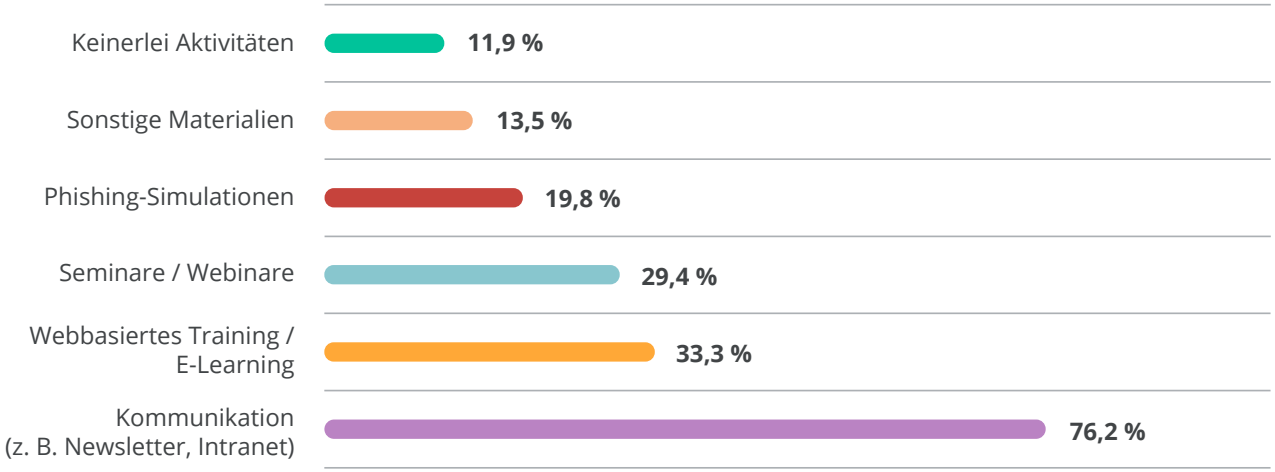




Awareness-Maßnahmen: Viele haben den Bedarf erkannt

Der Großteil der befragten Expertinnen und Experten sowie Organisationen reagiert auf das erhöhte Aufkommen an menschenbasierten Angriffen durch die Einbeziehung der Nutzerinnen und Nutzer. Über drei Viertel der Befragten geben an, irgendeine Form der Kommunikation durchzuführen, zum Beispiel Intranetpostings oder Nachrichten an die Mitarbeitenden. Aktive und dauerhafte Awareness-Maßnahmen, die diesen Gefahren proaktiv begegnen, werden von den Organisationen aber bisher seltener und eher punktuell ergriffen. Nur ein Drittel der Befragten setzt bereits E-Learnings oder webbasierte Trainings ein und nur jede und jeder Fünfte Phishing-Simulationen. Ein positiver Befund: Nur ein kleiner Teil klammert die eigenen Mitarbeitenden in den Schutzbemühungen aus, circa 11 % verzichten auf jegliche Maßnahmen in diesem Bereich.

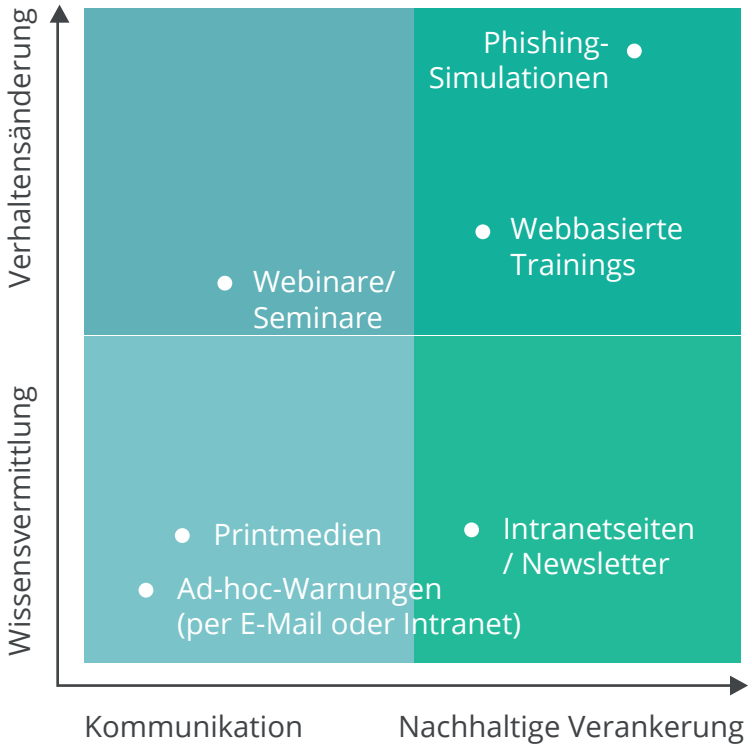
Mit welchen Maßnahmen steigern Sie die Awareness Ihrer Mitarbeitenden?



Die Ergebnisse entsprechen auch einem zugrundeliegenden Reifegradmodell der Cyber Security Awareness (siehe Abbildung S. 16), in dem Ein-Wege-Kommunikation (wie zum Beispiel durch Ad-hoc-Warnungen per E-Mail) ein einfacher und opportuner erster Schritt ist. Während solche Maßnahmen schnell und ohne großen Aufwand umsetzbar sind, sind sie dennoch eher reaktiver Natur und müssen durch Fachpersonal umgesetzt werden, das insbesondere im Bereich der IT-Sicherheit knapp ist.

Im Zuge der Erweiterung der Awareness-Maßnahmen stehen daher vermehrt Maßnahmen und Tools im Vordergrund, die es Organisationen ermöglichen, Security-Awareness und -Training in die laufenden Prozesse zu verankern, zum Beispiel über kontinuierliche Maßnahmen und die Orientierung an Daten und KPIs. So verschiebt sich der Fokus zudem in Richtung einer proaktiven Risikominimierung durch nachweisbare Verhaltensänderung von Mitarbeitenden, wie zum Beispiel das vermehrte Erkennen und Melden von verdächtigen E-Mails. Größere Unternehmen oder solche mit einem höheren Reifegrad setzen daher zunehmend interaktive und digitale Trainings oder aktive Maßnahmen wie Phishing-Simulationen ein, die auf das Verändern von Verhalten statt lediglich auf die Vermittlung von Informationen zielen.

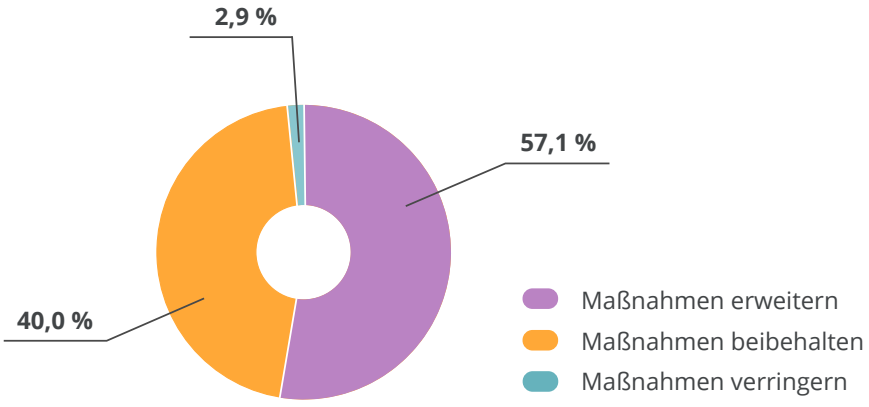
Verschiedene Awareness-Maßnahmen vor dem Hintergrund Ihrer Zielfunktion



Die Zeichen stehen auf Wandel

Ein Lichtblick: Fast sechs von zehn Befragten möchten ihre Maßnahmen zur Sensibilisierung der Mitarbeitenden in Zukunft ausbauen, immerhin 40 % ihre derzeitigen Maßnahmen beibehalten. Der Großteil der Befragten scheint sich also der Relevanz der Thematik bewusst zu sein. Dass bei der Umsetzung der Sicherheitsambitionen noch Nachholbedarf besteht, steht mit einem Blick auf die Ergebnisse außer Frage.

Wie ist Ihre Planung in puncto Sensibilisierung Ihrer Mitarbeitenden?



Infobox

Prävention im Bereich IT-Sicherheit ist Chefsache

Ein Fall, der für Aufsehen sorgte: Nach einem 40 Millionen Euro teuren CEO Fraud verklagte der Automobilzulieferer Leoni den Ex-Chef Dieter Bellé auf Schadenersatz. Dieses Vorgehen hebt die besondere Verantwortung der Geschäftsleitung für das Thema IT-Sicherheit und Datenschutz abermals deutlich hervor.

Dass ausreichende Prävention auch Haftungsimplikationen haben kann, erklärt sich aber bereits mit einem Blick auf die entsprechenden Rahmenbedingungen, vorgegeben etwa durch die DSGVO. Die IT-Sicherheits-Norm ISO-27001 hält Organisationen sogar dazu an, laufende Social-Engineering-Simulationen durchzuführen. Kommt es tatsächlich zu Vorfällen – wie im verlustreichen Fall von Leoni – müssen Unternehmen die Einhaltung dieser Verpflichtungen nachweisen. Im Zweifel haftet die Geschäftsführung für das Versäumnis, entsprechende präventive Maßnahmen eingeleitet zu haben.

Warum Airbags nicht vor Unfällen schützen – die Wichtigkeit des Faktors Mensch in der IT-Sicherheit

Ein Interview mit Bert Skaletski, CISO bei Merck KGaA

Bert Skaletski ist Chief Information Security Officer bei dem Wissenschafts- und Technologieunternehmen Merck KGaA. Als langjähriger Experte im Sicherheits- und Risikomanagement (z. B. CISM, CISSP) ist er für die weltweite Sicherheitsstrategie und -maßnahmen der gesamten Merck Group zuständig und betreut so auch den Aufbau der Security Awareness unter den 57.000 Mitarbeitenden in über 60 Ländern.

Wenn man sich die Cyber-Bedrohungslandschaft anschaut, scheint der Faktor Mensch eine Schlüsselrolle zu spielen. Warum können wir uns immer noch nicht auf technische Barrieren verlassen?

Viele Menschen denken, dass Technologien die Lösung für all unsere derzeitigen Probleme und Gefahren im Bereich IT-Sicherheit sind. Ich denke aber nicht, dass das in absehbarer Zeit der Fall sein wird. Die Angreifenden passen ihre Techniken, Taktiken und Prozesse laufend an, und in der Verteidigungsposition müssen wir schnell darauf reagieren. Worum es jetzt und auch in Zukunft geht, ist, Risiken zu managen – sowohl in Bezug auf ihre Wahrscheinlichkeit als auch auf ihre potenziellen Auswirkungen. Wenn wir uns dem Thema aus dieser Sichtweise nähern, kommt es letztlich immer auch auf den Faktor Mensch an, denn schließlich werden die Maschinen, über die wir sprechen, auch von Menschenhand erschaffen.

Ich vergleiche IT-Sicherheit gern mit Beispielen aus der Automobilwelt. Wir bauen und kaufen Autos bereits mit einer auf Unfälle ausgerichteten Ausstattung: Airbags, EPS, ABS, automatische Bremsen und so weiter.

Aber auch Autos mit der neuesten Technik – im Cyber-Security-Bereich wären das zum Beispiel Antivirenprogramme und Advanced Email Gateways – werden uns nicht davon befreien, weiterhin vorsichtig zu fahren. Der Staat hält uns sogar dazu an, Fahrstunden zu nehmen und eine Fahrprüfung abzulegen. Warum sollten wir die Menschen also nicht auch zu bestimmten „Verkehrssituationen" in der IT-Sicherheit schulen, damit wir das Risiko eines „Unfalls" minimieren? Weder Technologien noch unser Verhalten werden uns vollumfänglich schützen können. Wenn wir aber beide Faktoren miteinander kombinieren, reduzieren wir die Risiken so weit, dass wir damit umgehen und arbeiten können.

Warum wird Prävention auch weiterhin so wichtig sein?

Fakt ist: Technologien verändern sich immer schneller, und die Angreifenden werden uns immer einen Schritt voraus sein, um Schlupflöcher und Hintertürchen aufzuspüren. Wir hatten erst kürzlich einen Fall, bei dem sich einer unserer Mitarbeitenden über eine simulierte Phishing-Mail beschwerte, weil sie anders und wohl komplexer als die E-Mails zuvor war. Aber es ist eben genau diese Art von Training, die wir brauchen! Die Angreifenden ändern laufend ihre Vektoren. Das zwingt uns dazu, besonders vorsichtig und vorausschauend zu sein und in Schulungen auch Angriffe vorwegzunehmen, die in der Realität noch nicht aufgetaucht sind. Aber auch hier sei gesagt: Es geht um die Weiterentwicklung von Technologie und menschlichem Verhalten zugleich. Ich glaube fest an die Prämisse „immer updaten" und dass dies auch weiterhin eines unserer Leitprinzipien im Bereich IT-Sicherheit bleiben wird.

Während der COVID-19-Pandemie haben Cyberkriminelle mit Angst und Unsicherheit der Menschen gespielt. Welche Herausforderungen haben Sie bei Merck gesehen?

Viele Mitarbeitende hatten noch nie zuvor von zu Hause gearbeitet, wir mussten also zunächst für die nötige technische Infrastruktur sorgen. Die Angreifenden veränderten sehr schnell ihre Phishing-Kampagnen und passten sie an die Ängste während der COVID-19-Pandemie an. Deshalb haben wir auch unsere Cyberabwehr und unsere Awareness-Kampagnen aufgestockt, darunter spezifische Phishing-Simulationen.

Welche Fähigkeiten brauchen Führungspersonen und Mitarbeitende Ihrer Meinung nach in Zukunft, um sich dem „New Normal" anzupassen?

Die Angreifenden investieren viel Zeit darein, ihre Zielobjekte auszuwählen. Dabei geraten nicht immer nur Führungspersonen in den Fokus. Sie konzentrieren sich oft auf weniger gut geschulte Angestellte, um sie zu unbedachten Klicks auf E-Mails zu verleiten. Deshalb ist es unumgänglich, alle Mitarbeitenden gleichermaßen zu trainieren, nicht nur Führungskräfte. Wir müssen alle mit gesundem Menschenverstand und einem gewissen Maß an Misstrauen und Skepsis an Phishing-Mails herangehen. Ich betone immer, dass eine E-Mail, die zu gut ist, um wahr zu sein, genau das wahrscheinlich auch ist. Nur wenn wir Mitarbeitende über alle Hierarchien hinweg für die Gefahren sensibilisieren, können wir gefährliche Wissenslücken schließen.

In der Psychologie spricht man hier von Heuristik. Die Menschen müssen ein Gefühl für potenziell gefährliche Situationen entwickeln und in der Lage sein, mit ihren Mitteln schnell zu reagieren.

Genau. Aber es ist nicht ganz einfach, die Menschen dafür zu trainieren, nicht emotional oder impulsiv zu handeln, wenn sie beispielsweise eine bestimmte Betreffzeile lesen. Für Angreifende ist es beispielsweise sehr erfolgversprechend, User dazu zu drängen, Anmeldedaten zu aktualisieren und in ein Formular einzutragen. Wenn ich mich mit Kolleginnen und Kollegen aus der Branche unterhalte, sind wir uns einig, dass genau diese Attacken, die die Emotionen der Endnutzerinnen und -nutzer ausnutzen, am erfolgreichsten sind. Der Schluss, den ich daraus ziehe: Wir müssen neue Wege finden, die User für solche Szenarien zu trainieren.

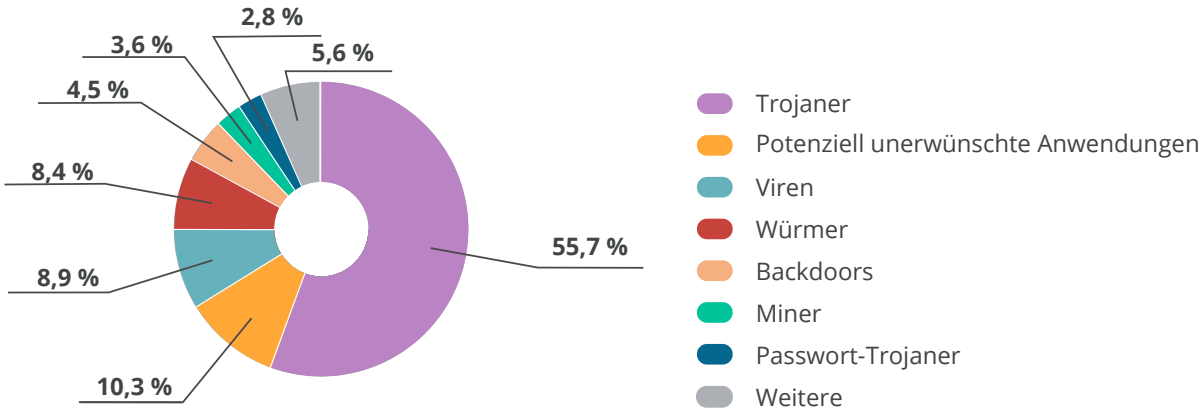
Müssen wir uns darauf einstellen, dass es in Zukunft noch schwieriger werden wird, Angriffe zu erkennen?

Definitiv. Aber wie bereits angesprochen, werden uns ein gesunder Menschenverstand und eine gesunde Portion Misstrauen und Skepsis dabei helfen, die Herausforderungen zu meistern. Wir sollten eine Balance zwischen regelmäßigen Updates auf der einen Seite und nachhaltigem Mitarbeitenden-Training auf der anderen Seite finden. Aus meiner Sicht ist Letzteres auf jeden Fall der Schlüssel zum Erfolg. Die traditionelle Schulbildung ist das eine, die hört irgendwann auf. Aber Lernen begleitet uns unser Leben lang. Das macht Schulungen so essenziell, vor allem im Bereich IT-Sicherheit, der von vielfältigen und dynamischen Angriffstechniken und -taktiken geprägt ist.

Malware:
Der dramatische Anstieg im Überblick

Mehr als die Hälfte der erkannten Malware-Typen sind Trojaner

Häufigkeitsverteilung verschiedener Malware-Typen



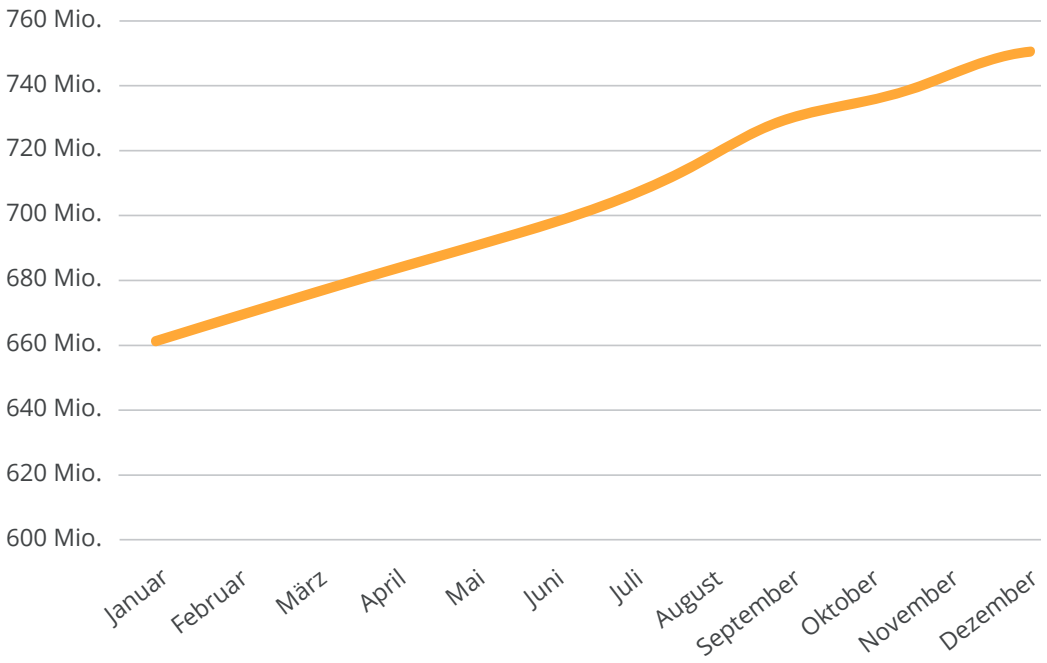
Wie die Auswertungen aus der AV-ATLAS-Datenbank (Datensatz 1) zeigen, sind auch 2020 Trojaner wie Ryuk und Egregor die am häufigsten genutzte Schadsoftware gewesen. Ihre Komplexität macht sie besonders gefährlich: Versteckt auf Webseiten, in E-Mails, in Software oder in Dateien, spielen sie weitere Schadsoftware auf das Gerät, verschlüsseln Daten oder installieren Bots und Krypto-Miner. Sie lassen sich durch ihren oftmals polymorphen Schadcode nur schwer mit Secure Email Gateways identifizieren und abblocken. Gleichzeitig verwenden die Angreifenden häufig Taktiken (zum Beispiel die Ausführung von Office-Makros), die gezielt darauf ausgerichtet sind, technische Barrieren zu umgehen. Das verdeutlicht umso mehr die Bedeutung einer Human Firewall – also einer Belegschaft, die mit IT-Sicherheitsrisiken umzugehen weiß.

Trojaner sind auch 2020 die am häufigsten genutzte Schadsoftware gewesen.

Die starke Position von Trojanern – sie machen mehr als die Hälfte der gesamten Menge an Malware aus – lässt vermuten, dass Social Engineering und Ransomware auch weiter auf dem Vormarsch sind. Denn oftmals wird beim Einsatz von Ransomware, auch als Erpressungstrojaner bekannt, gezielt mit den Emotionen der Opfer gespielt. Aber auch Potentially Unwanted Applications (PUA), klassische Viren und Würmer, sind weiterhin verbreitet. Zu PUA zählen hierbei etwa Adware und Spyware, die mehr als 10 % der entdeckten Malware ausmachen. Auch wenn der Schaden hier nicht unmittelbar ersichtlich ist, können Daten von Nutzenden im Anschluss für unerwünschte Zwecke missbraucht werden. Immer häufiger treten die verschiedenen Arten von Malware zudem auch gebündelt auf.

Die Menge an neuer Malware erreicht neue Dimensionen

Anzahl der erkannten Malware-Typen in 2020



2020 hat die Gesamtmenge an neuer Malware ebenfalls einen gefährlichen Höhepunkt erreicht: Im Schnitt liegt die Entwicklungsrate neuer Malware-Typen bei 4,2 Samples pro Sekunde. Bis zum Ende des Jahres 2020 wurden so insgesamt über 750 Millionen neue Schadprogramme erkannt. Der Anstieg an Malware und Massen-Malware ist dabei kontinuierlich zu beobachten.[22]

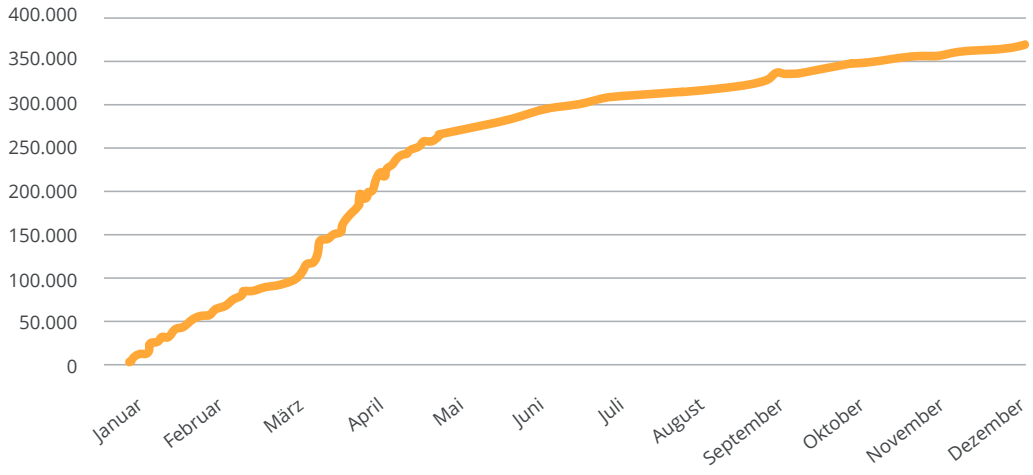
Im Schnitt liegt die Entwicklungsrate neuer Malware bei 4,2 Stück pro Sekunde.

Ein Blick auf die AV-TEST-Daten zur Entwicklung aus den vorherigen Jahren verdeutlicht die Dimensionen der Entwicklung. Im Jahr 2016 wurden 127,5 Millionen Neuentwicklungen verzeichnet, 2017 waren es 121,7 Millionen neue Schadprogramme.[23] So wurde 2020 eine noch nie da gewesene Gesamtmenge an neuer Malware erreicht – und die Dunkelziffer dürfte noch weitaus höher liegen.

[22] AV-TEST - The Independent IT-Security Institute (2020). Security Report 2019/2020.
[23] AV-TEST - The Independent IT-Security Institute (2018). Security Report 2017/2018.

Die COVID-19 Pandemie befeuert die Entwicklung von Ransomware

Anzahl neu erkannter Ransomware in 2020



Die Entwicklungsdynamik neuer Ransomware im Jahr 2020 macht vor allem eines deutlich: Cyberkriminelle sind immer am Puls der Zeit. Gerade zwischen März und Mai 2020 war ein extrem starkes Wachstum an neuer Ransomware zu verzeichnen. Die Hacker nutzten ganz offensichtlich die allgemeine Verunsicherung durch die COVID-19-Pandemie aus und steigerten ihre Aktivitäten enorm. Beeindruckend ist dabei die Geschwindigkeit. Der dramatische Anstieg an neuer Ransomware fällt nahezu zeitgleich mit dem Beginn des ersten Lockdowns in weiten Teilen Europas zusammen.

Die Hacker nutzen den allgemeinen Wandel und die Veränderungen, bedingt durch COVID-19, aus und entwickeln Ransomware, die inhaltlich passend auf die Pandemie zugeschnitten ist.

Die Cyberkriminellen scheinen also in der Lage zu sein, ohne große Verzögerung auf neue Umstände wie einen gesellschaftlichen Wandel, neue Technologien oder auch auf eine weltweite Pandemie, zu reagieren. Diese Beobachtung macht einmal mehr deutlich, dass allgemeiner und zeitgerechter Prävention, unter anderem auch durch die Sensibilisierung von Mitarbeitenden, eine besondere Bedeutung zukommt.

Infobox

Schutzfaktor Flurfunk - die Organisationsstruktur als Einflussfaktor?

Viele der inhaltlichen und psychologischen Taktiken im Social-Engineering-Bereich drehten sich 2020 um Homeoffice und das Coronavirus. Darüber hinaus stellt sich aber die Frage, ob Homeoffice an sich beziehungsweise die Organisationsstruktur der Unternehmen bereits ein erhöhtes Risiko für Social-Engineering-Angriffe darstellt. Um dieser Fragestellung auf den Grund zu gehen, hat SoSafe bereits 2019 in einer Analyse verschiedene Organisationstypen miteinander verglichen: zentral aufgestellte Organisationen, bei denen alle Mitarbeitenden an einem Ort arbeiten und häufig in Großraumbüros zusammensitzen, und dezentrale Organisationen, die das Arbeiten im Homeoffice als üblichen Arbeitsmodus eingeführt hatten. In beiden Fällen wurden vergleichbare Phishing-Mails mit vergleichsmäßig niedrigem Schwierigkeitsgrad an alle Mitarbeitenden versendet.

Die Ergebnisse zeigen, dass die dezentralen Organisationen eine um das Dreifache erhöhte Klickrate von durchschnittlich 30 % aufweisen. Im Vergleich dazu klicken die Mitarbeitenden in zentralen Organisationen mit 12 % deutlich seltener. Die Analyse legt den Verdacht nahe, dass zentral aufgestellte Organisationen etwas besser gegen Social-Engineering-Angriffe abgesichert sind. Ein Grund dafür könnte sein, dass Mitarbeitende sich in Büros öfter zu verdächtigen E-Mails austauschen. Man könnte auch sagen: Der Flurfunk schützt. In der aktuellen Situation, in der fast alle Organisationen auf Homeoffice setzen, ist es daher besonders wichtig, die Mitarbeitenden für Phishing-Mails zu sensibilisieren und so das vermeintlich höhere Risiko im Homeoffice präventiv zu adressieren.

Psychologische und technische Vektoren – die Risikofaktoren im Überblick

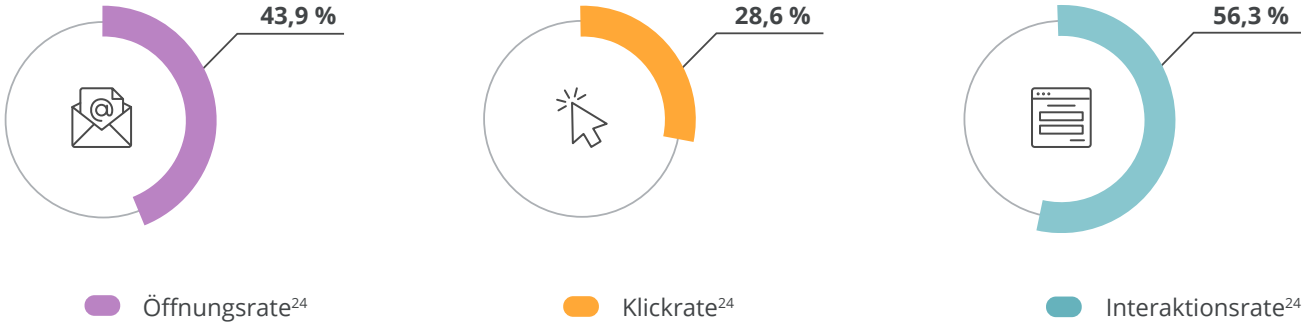
Klicken, Öffnen, Interagieren: Zahlen lassen auf hohes Human Risk schließen

Die Ergebnisse der SoSafe Awareness-Plattform (Datensatz 2) aus dem Jahr 2020 zeigen: Das Angriffspotenzial beziehungsweise die Erfolgswahrscheinlichkeit für Phishing-Angriffe ist enorm.

Ein Großteil der Mitarbeitenden in Organisationen ist zunächst nicht in der Lage, schädliche E-Mails zu erkennen.

Wurde noch keine systematische Awareness-Maßnahme (zum Beispiel in Form von Phishing-Simulationen oder webbasierten Trainings) durchgeführt und etabliert, öffnet fast jede und jeder zweite Nutzende Phishing-Mails. Von diesen Usern klicken fast 30 % auf in der E-Mail enthaltene Links oder Anhänge. 57 % der Nutzenden interagieren zudem mit simulierten E-Mails, die Elemente wie fingierte Formulare enthalten oder auf diese verlinken – geben also beispielsweise Anmeldeinformationen oder persönliche Daten in gefälschte Login-Masken ein.

Das zeigt eindrücklich, dass ein Großteil der Mitarbeitenden in Organisationen zunächst nicht in der Lage ist, schädliche E-Mails zu erkennen. So können sie ihre Organisation durch einen unvorsichtigen Umgang mit Phishing-Mails in eine ernst zu nehmende Gefahrenlage bringen.



Diese technischen Vektoren provozieren die meisten Klicks auf Phishing-Mails

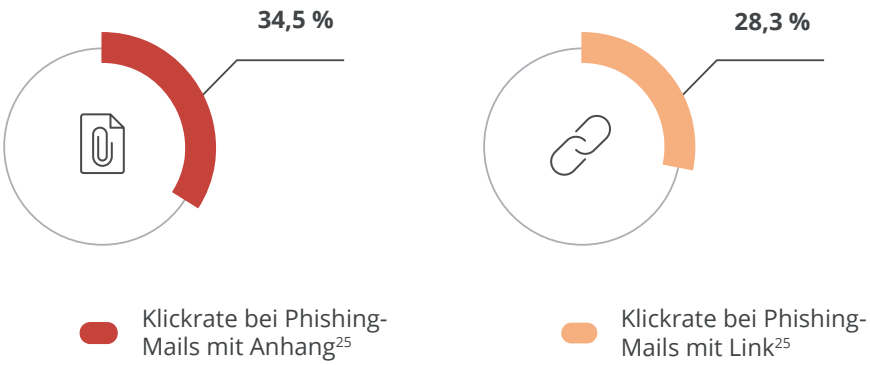
Bei den Vektoren zeigt sich, dass mit durchschnittlich fast 35 % die Klickrate am höchsten ist, wenn die simulierten Phishing-Mails einen Anhang enthalten.

Am erfolgreichsten sind Phishing-Mails mit schadhaften Anhängen – mehr als ein Drittel der Empfängerinnen und Empfänger klicken.

Aber auch die Verwendung von Links regt fast ein Drittel der Empfängerinnen und Empfänger zum Klick an. Es scheinen also gerade solche E-Mails, die eine interessante Interaktion versprechen, ins Schwarze zu treffen.

[24] Datengrundlage: 1,4 Mio. simulierte Phishing-Angriffe aus der SoSafe Awareness-Plattform.

Klickraten nach ausgewählten technischen Vektoren

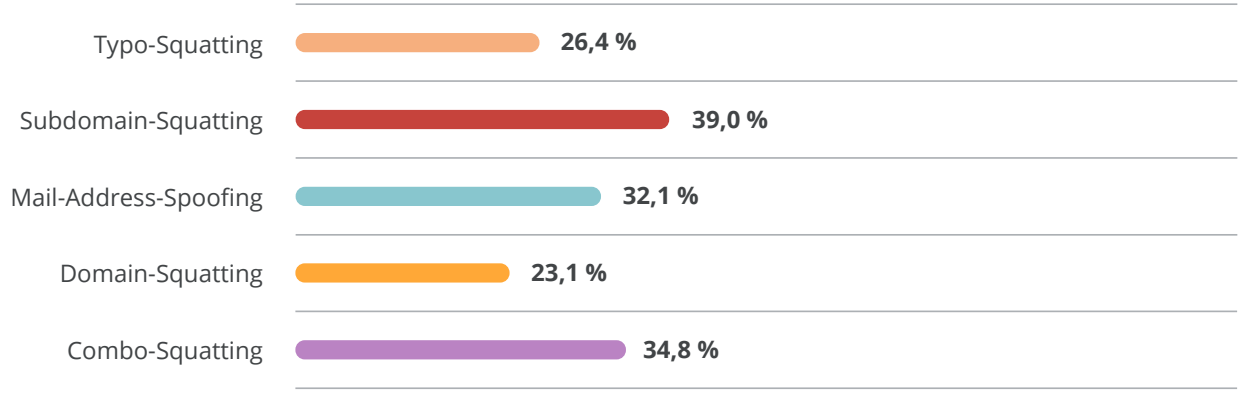


Gerade neuartige Techniken zur Adressmanipulation sind erfolgreich

Häufig manipulieren Angreifende Absenderadressen, um die Erfolgswahrscheinlichkeit ihrer Angriffe zu optimieren. Beispielsweise werden beim sogenannten „Domain-Squatting" ähnliche Domains zur Zieldomain registriert, zum Beispiel amozon.com bei einem Angriff, welcher einen Absender aus der Domain amazon.de imitieren soll. Auch klassisches „Spoofing" kommt weiterhin zum Einsatz, indem der Absender im E-Mail-Header überlagert wird. Wenn man sich verschiedene Techniken der Manipulation, die die SoSafe Plattform bei simulierten Angriffen verwendet, anschaut, sind gerade komplexere Techniken sehr erfolgreich. So werden E-Mails, die „Subdomain-Squatting" verwenden, von beinahe 40 % der Empfängerinnen und Empfänger angeklickt.

Auch das sogenannte „Combo-Squatting" führt zu einer Klickrate von fast 35 %. Beim „Subdomain-Squatting" wird ein Begriff der Zieldomain vor eine unscheinbare Top-Level-Domain gesetzt, beim „Combo-Squatting" im Rahmen einer ganz neu erstellten Domain neben anderen Begriffen verwendet. Eine genauere Erläuterung verschiedener Manipulationsmethoden führt auch das SoSafe Cyber-Security-Glossar (www.sosafe.de/glossar/) auf.

Klickraten bei Techniken zur Adressmanipulation[25]



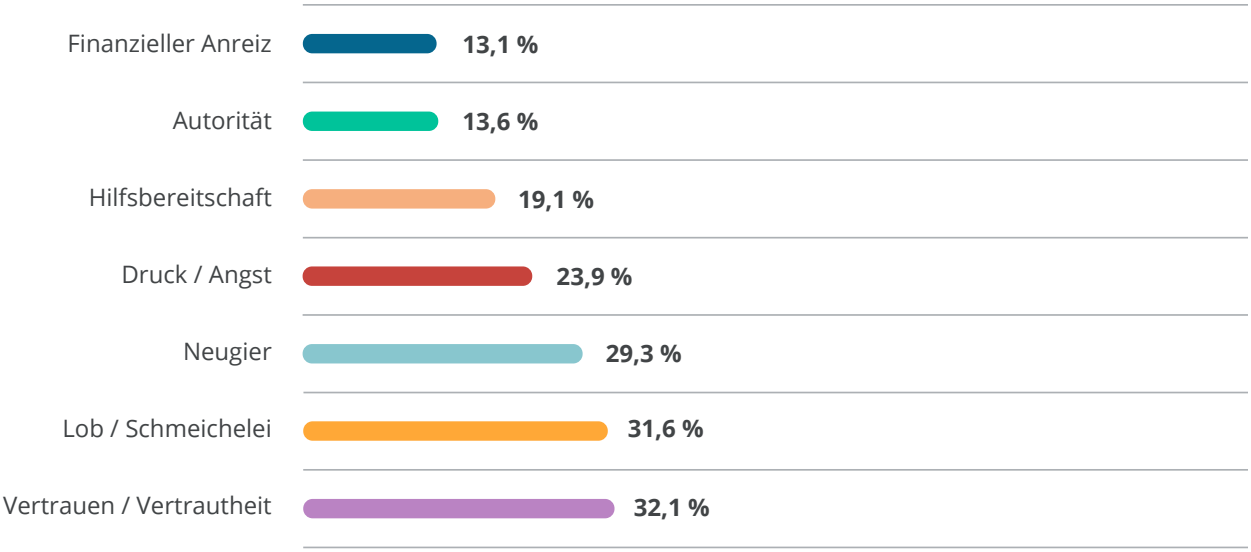
[25] Datengrundlage: 1,4 Mio. simulierte Phishing-Angriffe aus der SoSafe Awareness-Plattform.

Bei diesen psychologischen Tricks wird am meisten geklickt

Immer mehr Cyberkriminelle manipulieren ihre Opfer gezielt über psychologische Tricks – ein Vorgang, den man unter Social Hacking oder Social Engineering subsummiert. Die SoSafe Expertinnen und Experten beschäftigen sich daher mit Fragen rund um die Psychologie des Hackings: Was sind die erfolgreichsten Phishing-Maschen? Welcher psychologischen Mechanismen bedienen sich die Cyberkriminellen? Wie verändern sich die Phishing-Maschen, orientiert am Zeitgeschehen?

Angreifende setzen in diesem Kontext auf ein breites Set an psychologischen Taktiken, die die unterschiedlichsten menschlichen Emotionen adressieren, darunter Stress, Angst, Autoritätsglaube oder Neugier. Die SoSafe Awareness-Plattform ist in der Lage, die Erfolgsrate dieser diversen Taktiken zu bewerten, indem Angriffe kategorisiert und mit Tags versehen werden. In der Gesamtschau gibt dies eine interessante Perspektive auf die erfolgreichsten psychologischen Taktiken.

Klickraten nach psychologischen Taktiken[26]



Es klickt fast jede und jeder Dritte, wenn die E-Mail eine vertrauensvolle Beziehung vorspielt oder der Adressatin oder dem Adressaten schmeichelt.

Dabei wird auf den ersten Blick klar, dass Phishing-Mails, die auf das Erwecken von positiven Emotionen wie Vertrauen setzen, die Empfängerinnen und Empfänger eher in die Falle locken als solche, die negative Gefühle wie Druck und Angst hervorrufen. So klickt fast jede und jeder Dritte, wenn die E-Mail eine vertrauensvolle Beziehung vorspielt oder der Adressatin oder dem Adressaten schmeichelt.

[26] Datengrundlage: 1,4 Mio. simulierte Phishing-Angriffe aus der SoSafe Awareness-Plattform.

Ebenfalls besonders hoch sind die Klickraten, wenn die Inhalte die Opfer des Phishing-Angriffs neugierig machen sollen.

Die Kombination aus Neugier und Thematisierung der COVID-19-Pandemie animiert 2020 am ehesten zum Klick auf potenziell schädliche E-Mails.

Hinter dem Faktor Neugier stecken 2020 viele simulierte Phishing-Mails, die das Thema Corona beinhalten – so wie es sich auch in freier Wildbahn beobachten ließ. Die beiden am häufigsten geklickten Betreffzeilen der SoSafe Phishing-Simulation veranschaulichen die Masche eindrücklich: Die Kombination aus Neugier und Thematisierung der COVID-19-Pandemie animiert 2020 am ehesten zum Klick auf potenziell schädliche E-Mails. Die beschriebenen Corona-Mails wiesen mit bis zu 78 % teilweise eine stark erhöhte Klickrate auf (siehe Betreffzeilen-Analyse S. 29).

E-Mails, die hingegen Stress und Zeitdruck aufbauen sollen, führen nur ein Viertel der Empfängerinnen und Empfänger hinters Licht. Mit einer durchschnittlichen Klickrate von 13 % lassen sich Mitarbeitende am seltensten von finanziellen Versprechungen oder Scam täuschen. Traditionelle Phishing-Betreffzeilen wie „Sie haben den Jackpot gewonnen“ scheinen ihre ehemals starke Wirkung also nicht weiter aufrechterhalten zu können.

Top-10-Betreffzeilen 2020

Die Analyse der am häufigsten geklickten Betreffzeilen aus dem Jahr 2020 zeigt noch einmal detaillierter, welche emotionalen Manipulationsversuche am wirkungsvollsten waren.[27] So finden sich, wenig überraschend, viele coronaspezifische Themen unter den erfolgreichsten Angriffsversuchen. Interessant dabei ist allerdings, dass die COVID-19-Thematik von den Angreifenden auf unterschiedliche Art und Weise ausgenutzt werden kann.

1. **Agenda für das Meeting nächste Woche**

Agenda für das Corona-Meeting nächste Woche

2. **Lieferabläufe zur Corona-Krise - Sendung 5380499815 nicht zugestellt**

3. **Konto: Bitte authentifizieren Sie Ihr Konto.**

4. **Server Migration - Datenprüfung erforderlich**

5. **Wichtig: Umstellung auf Office 365**

6. **Sicherheitshinweis: Neuer Evakuierungsplan**

7. **Interessanter Kandidat für Sie?**

8. **Wir Suchen Kandidaten wie Sie!**

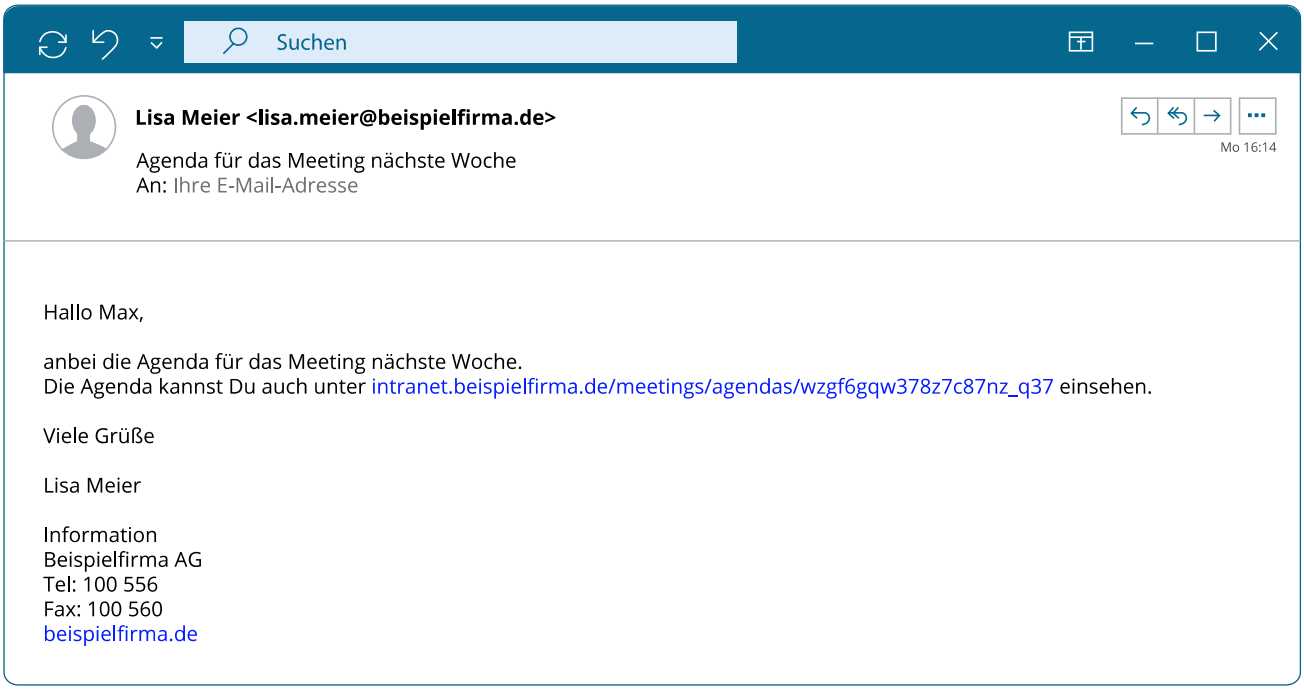
9. **Dringend: E-Mail-Kontingent aufgebraucht**

10. **Wichtig: Verlängerung Office 365**

[27] Datengrundlage: 1,4 Mio. simulierte Phishing-Angriffe aus der SoSafe Awareness-Plattform.

Platz 1 - 58,8 % Klickrate

Psychologische Taktiken: Routineanliegen / Autorität / Neugier



So simpel und doch so effektiv: Der Underdog der Betreffzeilen ist denkbar einfach gemacht, aber mit einer Klickrate von 58,8 % sehr wirkungsvoll. Bei dieser Social-Engineering-Masche wird auf gleich mehrere psychologische Faktoren gesetzt. Zunächst handelt es sich um ein sogenanntes Routineanliegen. Solche E-Mails landen bei vielen Mitarbeitenden wöchentlich im Postfach. Das ist besonders gefährlich, denn so sind sie weniger wachsam für mögliche Phishing-Anzeichen.

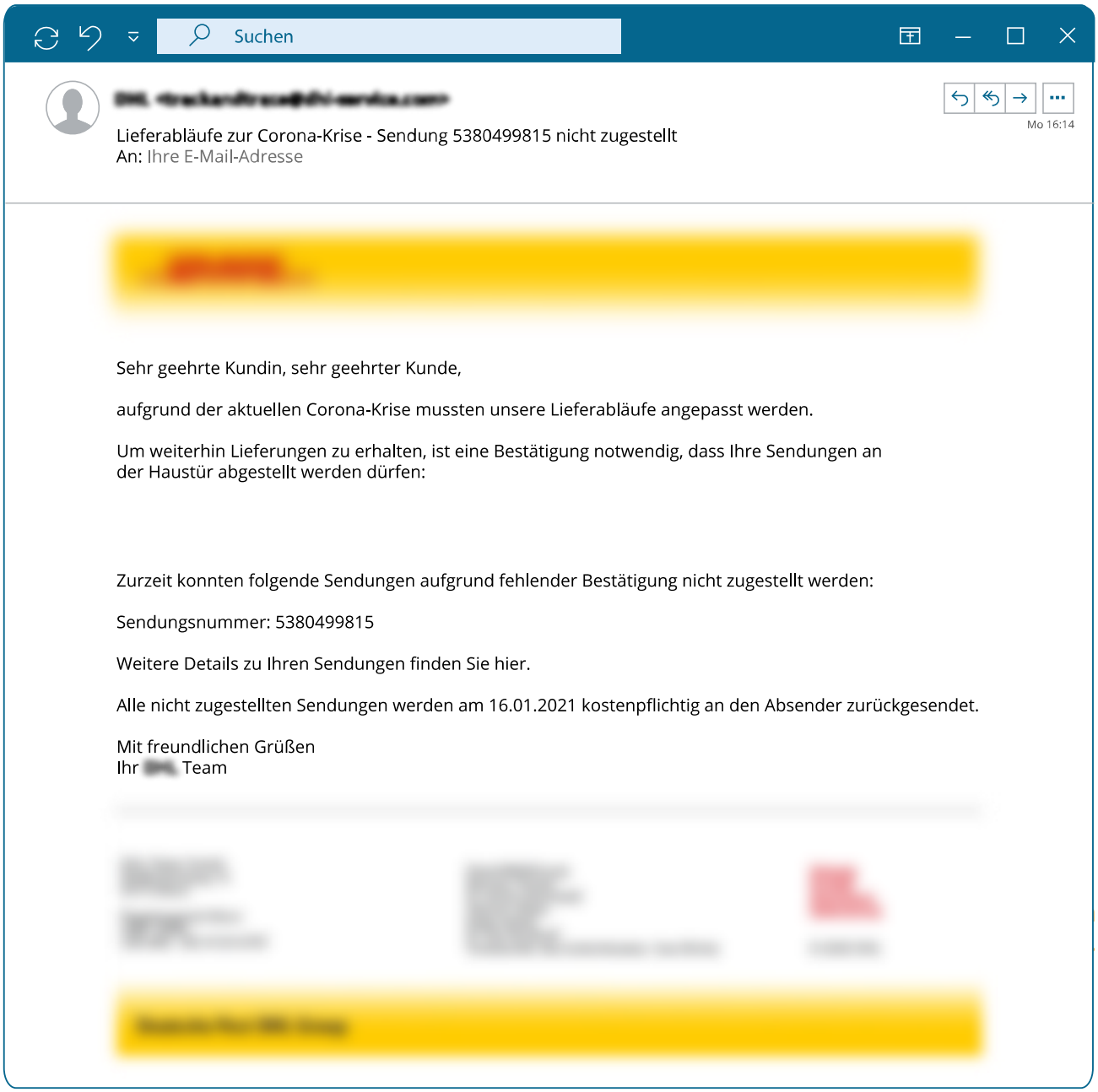
Durch die Nutzung des Wortes „Corona“ in der Betreffzeile erhöht sich die Klickrate teilweise um bis zu 50%.

Darüber hinaus nutzen Cyberkriminelle die natürliche Dynamik im Unternehmen aus. Denn die Vorbereitung auf anstehende Meetings gehört zu den täglichen Pflichten der Mitarbeitenden und bringt so einen gewissen Erfüllungsdruck mit sich. Zu guter Letzt spielt auch Neugier eine Rolle. Der drastische Wandel von Arbeitsprozessen – bedingt durch COVID-19 – hat ein erhöhtes Informationsbedürfnis mit sich gebracht. Insgesamt eine gefährliche Kombination, die diese Betreffzeile zu der am häufigsten geklickten Betreffzeile 2020 macht.

Besonders spannend: Während Angreifende im späteren Verlauf der Pandemie sehr gezielte Angriffsversuche entwickelten, konnten in der allerersten Phase des Ausbruchs sehr schnell auch einfache Anpassungen an bereits bestehenden Phishing-Kampagnen beobachtet werden. Vor diesem Hintergrund ist besonders interessant, dass die Klickrate dieser E-Mail durch das Einfügen des Wortes „Corona“ in der Betreffzeile auf 78,8 % gesteigert werden kann.

Platz 2 - 50,7 % Klickrate

Psychologische Taktiken: Neugier / Angst



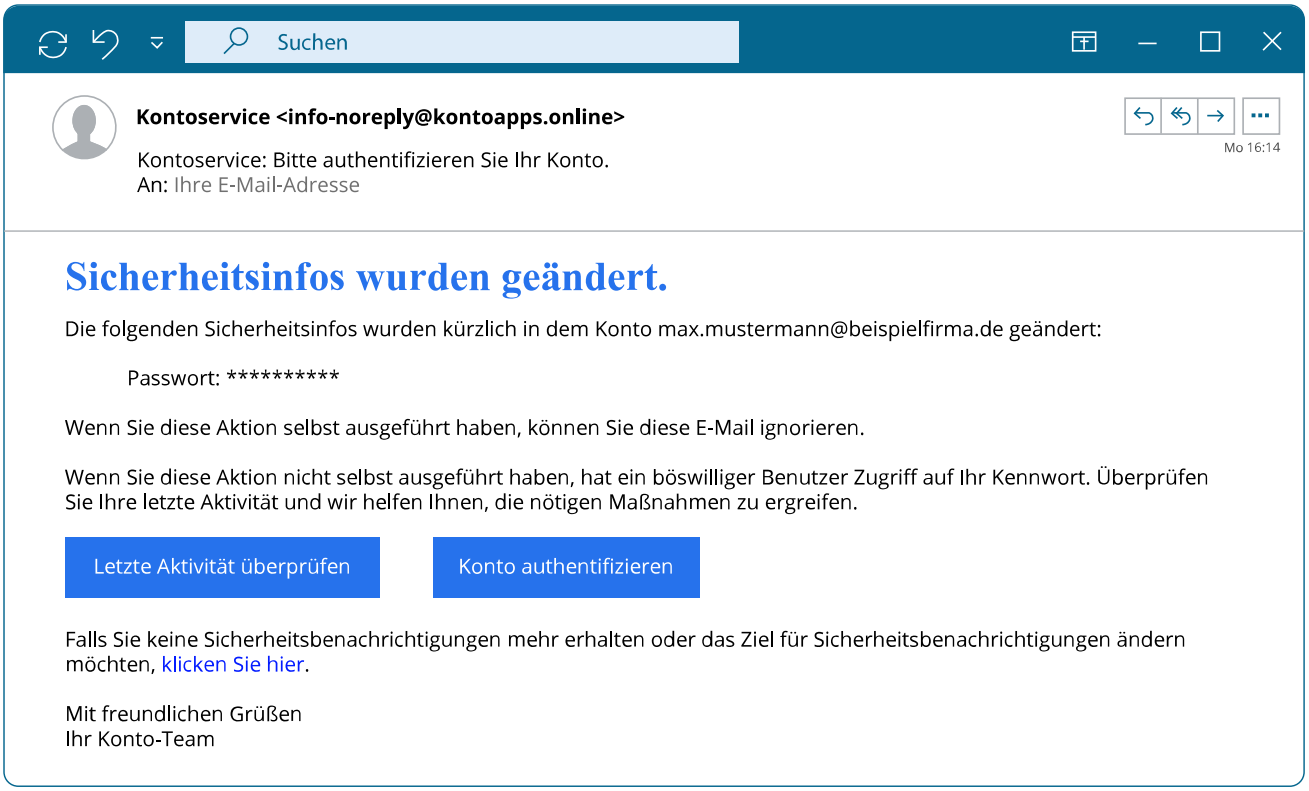
Hier wird das Topthema Corona kombiniert mit der menschlichen Neugier – eine Verbindung, die mit 50,7 % Klickrate sehr gut funktioniert. Bedingt durch landesweite Lockdowns und die geschlossenen Läden sind Onlinebestellungen allein im ersten Lockdown zwischen März und Mai um 20 % gestiegen.[28] Konsequenterweise versenden auch die Cyberkriminellen dazu passende Phishing-Mails.

Auch 2021 gilt noch die Devise: Immer skeptisch sein, wenn E-Mails im Zusammenhang mit COVID-19 im Posteingang landen.

Ein weiterer psychologischer Faktor, der hier zum Einsatz kommt, ist Angst. Besonders im Weihnachts-Shoppingstress kann das fehlende Geschenk für ein Familienmitglied schon einmal Panik auslösen. So ist es wenig erstaunlich, dass schadhafte Links oder Dateianhänge besonders schnell und unbedacht angeklickt werden. Dass derartige Betreffzeilen viele Mitarbeitende noch immer besonders neugierig machen, wissen auch die Hacker. Daher gilt auch 2021 noch die Devise: Immer skeptisch sein, wenn E-Mails im Zusammenhang mit COVID-19 im Posteingang landen.

Platz 3 - 45,4 % Klickrate

Psychologische Taktiken: Dringlichkeit / Verunsicherung[29]



[28] Bitkom (2020). Wie die Corona-Krise das Online-Shopping verändert.
[29] E-Mail-Beispiel geringfügig redigiert.

Aufgrund der Pandemie mussten viele Unternehmen spontan ins Homeoffice wechseln. Mehr oder weniger gut vorbereitet, kamen plötzlich zahlreiche neue Tools zum Einsatz, darunter Teams, Slack oder Zoom. Besonders viele Unternehmen migrierten aufgrund von vermehrter Remote-Arbeit zu Anbietern, die vielfältige Kollaborationsmöglichkeiten bieten.

Auch 2021 muss noch vermehrt mit Angriffen gerechnet werden, die sich auf gestohlene Anmeldeinformationen stützen.

Passend dazu tauchten Phishing-Mails auf, die genau dort angriffen und ausnutzten, dass viele Mitarbeitenden noch unvertraut mit den Lösungen und der Benutzeroberfläche waren. „Konto-service: Bitte authentifizieren Sie Ihr Konto" erzielte die dritthöchste Klickrate von 45,4 %. Die Kollaborationstools sind für Hacker ein attraktiver Weg in die Systeme von Unternehmen. Über sogenannte Credential-Theft-Angriffe, die auf das Erlangen von Login-Daten abzielen, erhalten sie Zugriff auf die Tools und damit häufig ebenfalls Zugang zu sensiblen Daten. Auch 2021 muss noch vermehrt mit Angriffen gerechnet werden, die sich auf gestohlene Anmeldeinformationen stützen.

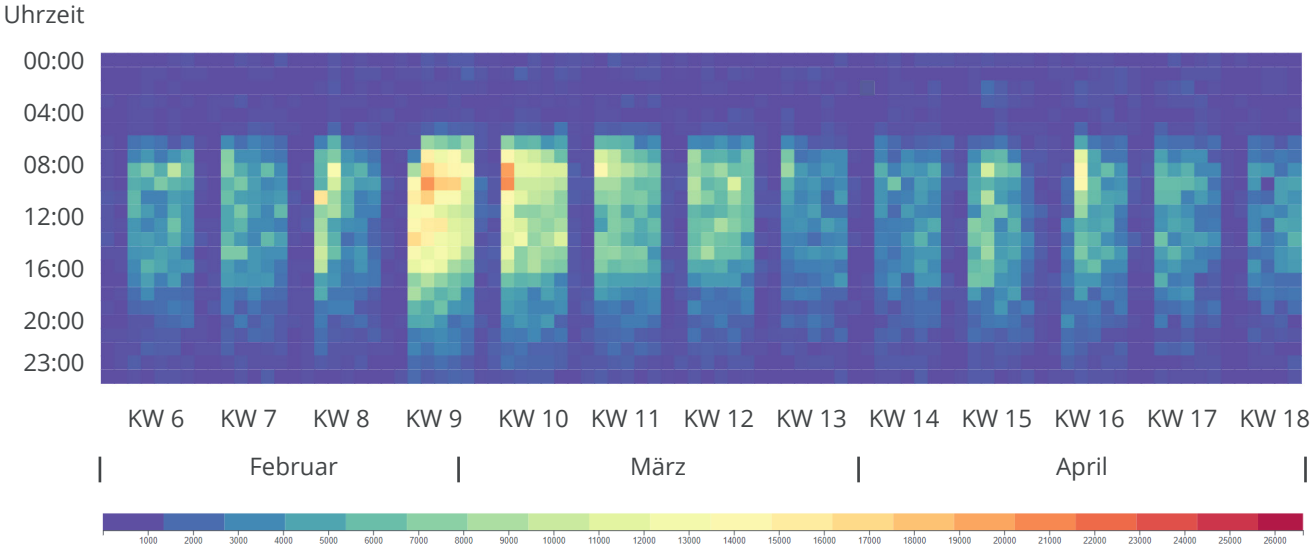
Besonders spannend: Bei Unternehmen, die die beschriebenen Tools bereits eingeführt hatten, war die Klickrate einer ganz ähnlichen E-Mail – eine, die die Verlängerung einer bereits eingesetzten Software thematisiert – mit 25,2 % wesentlich niedriger. Dies zeigt noch einmal, wie wichtig es ist, die Veränderung von Arbeitsprozessen und Tools mit entsprechenden Sensibilisierungsmaßnahmen zu begleiten.

Der unmittelbare Einfluss der COVID-19-Pandemie: Während des Lockdowns wurde besonders häufig geklickt

Ein Blick auf die zeitliche Dynamik stärkt die Vermutung, dass COVID-19 einen Einfluss auf die Erfolgswahrscheinlichkeit von Phishing-Angriffen hatte. Die Klickrate stieg mit dem ersten Lockdown im März 2020 rapide an, in einer Phase, in der wir besonders schutzlos waren.

Dies legt nahe, dass die Verunsicherung der Menschen in dieser Zeit den Umgang mit Cybergefahren beeinflusst hat und E-Mails in einer Situation hoher Verunsicherung – und gerade im neuartigen Homeoffice-Setting – besonders unbedarft angeklickt wurden. Hinzu kommt, dass sich gerade in dieser Phase die verwendeten Phishing-Templates oftmals direkt auf Corona oder veränderte Arbeitsbedingungen im Zuge des pandemischen Geschehens bezogen hatten.

Klicks auf Phishing-Mails zwischen Februar und März 2020[30]



[30] Datengrundlage: 1,4 Mio. simulierte Phishing-Angriffe aus der SoSafe Awareness-Plattform.

Fraunhofer FKIE

Präventive und reaktive Cyber Security Awareness – IT-Sicherheit als Gemeinschaftsprojekt

Ein Interview mit Prof. Michael Meier, Leiter Cyber Security Fraunhofer FKIE

Prof. Dr. Michael Meier ist Inhaber des Lehrstuhls für IT-Sicherheit am Institut für Informatik der Universität Bonn und Leiter der Abteilung Cyber Security am Fraunhofer FKIE. Seine Forschungsinteressen liegen im Bereich der angewandten Aspekte von IT-Sicherheit mit dem Schwerpunkt auf Angriffs- und Malware-Analyse sowie -Erkennung. Michael Meier ist außerdem Gründungsmitglied und Sprecher der Fachgruppe Security - Incident Detection and Response (SIDAR) der Gesellschaft für Informatik e.V., Co-Chair der internationalen Tagung Detection of Intrusions & Malware and Vulnerability Assessment (DIMVA) sowie Vorstandsmitglied der Gesellschaft für Datenschutz und Datensicherheit (GDD). Er ist Mitgründer des Security-Start-ups Identeco.

Während der COVID-19-Pandemie konnte man einen starken Anstieg von Phishing-Kampagnen beobachten. Was, glauben Sie, sind die Gründe dafür?

Wir waren und sind während der Pandemie alle mit viel Ungewohntem konfrontiert – das bringt an vielen Stellen auch große Unsicherheiten mit sich. Unsere Arbeitsweisen ändern sich teils sehr spontan, und es bleibt wenig Zeit, sich an neue Abläufe zu gewöhnen – sie müssen ad hoc neu erfunden werden. Genau diese Verunsicherung machen sich Phisher zunutze. Denn sie erleichtert es ihnen, IT-Nutzerinnen und -Nutzer vom richtigen Pfad abzubringen.

Das Jahr 2020 hat uns so auch noch einmal verdeutlicht, wie wichtig Prävention und Flexibilität sind – auch im Bereich IT-Sicherheit. Welche Themen und Trends, vielleicht sogar neue Forschungsansätze haben Sie aus dem letzten Jahr mitgenommen?

Viele Menschen nutzen seit dem vergangenen Jahr verstärkt Onlinedienste, manche sogar zum ersten Mal. Neben der allgemeinen Verunsicherung gehen damit auch neue Herausforderungen im Bereich der Identitätsdatenverwaltung, insbesondere bei Passwörtern, einher. Gleichzeitig hat sich auch das allgemeine Bedrohungspotenzial durch Identitätsdiebstahl, sogenannte Credential-Theft-Angriffe, deutlich vergrößert. Cyberkriminelle haben diese neu entstandenen Sicherheitslücken schnell aufgespürt und ausgenutzt.

Wir haben uns dieser Thematik in den letzten Jahren bereits intensiver gewidmet und konnten 2020 passenderweise unser Projekt EIDI (Effektive Warnung nach digitalem Identitätsdiebstahl) abschließen. Ziel war und ist es, die Auswirkungen eines solchen Diebstahls zu begrenzen – etwa, wenn Passwörter für Onlinedienste gestohlen werden. Durch das neue Remote-Work-Setting haben die Forschungsergebnisse weiter an Relevanz gewonnen. Denn im Zusammenspiel mit präventiven Maßnahmen wie der Awareness von Mitarbeitenden kann man darüber das enorm gestiegene Risiko reduzieren. Unsere Ausgründung identeco.de bietet inzwischen entsprechende Sicherheitsdienstleistungen für alle interessierten Unternehmen an.

In dem Projekt „IT-Security Awareness Penetration Testing" (ITS.APT) haben Sie sich zum Ziel gesetzt, IT-Sicherheitsbewusstsein strukturell messbar zu machen. Warum ist es für Organisationen so wichtig, die Awareness ihrer Mitarbeitenden im Blick zu haben?

Es ist nicht nur wichtig, die Awareness der Mitarbeitenden im Blick zu haben, sondern diese auch konkret zu fördern. Dabei geht es einerseits um den präventiven Aspekt der Awareness, also um das Vermeiden von Fehlverhalten, damit die Erfolgsquote von Phishing-Angriffen reduziert wird. Es gilt aber andererseits auch, den reaktiven Aspekt zu erfassen – Mitarbeitende sollten beim Entdecken und Melden von Auffälligkeiten mitwirken und so den Schaden begrenzen. Für den Fall, dass tatsächlich einmal versehentlich auf einen Link in einer Phishing-Mail geklickt wird, ist eine schnelle Reaktion Gold wert. Um ein Schiff sicher von A nach B zu bringen, braucht es letztlich viele Seeleute und nicht nur jemanden, der das Radar im Auge behält.

Welche Rolle wird der Faktor Mensch auch in Zukunft bei der Stärkung der IT-Sicherheit einnehmen?

Eine große. Denn IT-Sicherheit zielt auf die Absicherung von soziotechnischen Systemen, in denen Menschen mit Technik interagieren. Diese Interaktion erfordert Freiheiten – Freiheiten, die auch missbraucht werden können, wie aktuelle Cyberangriffe eindrücklich zeigen. Unserer Anstrengung, die IT-Sicherheit zu stärken, stehen immer neue Entwicklungen und Technologien gegenüber. Mit der zunehmenden Digitalisierung bieten wir also auch immer mehr Angriffsfläche. Dieser schnelllebige technische Fortschritt wird in absehbarer Zeit nicht abbrechen. Umso wichtiger ist es, mit der Entwicklung durch entsprechende Awareness-Maßnahmen Schritt zu halten, um Vorfälle zu vermeiden und schnell auf sie reagieren zu können.

Ihre Forschung beschäftigt sich mittelbar auch mit der Verbesserung des IT-Sicherheitsbewusstseins. Welche Ratschläge können Sie Organisationen mitgeben?

Wenn ich Organisationen etwas mitgeben darf, dann ist es Folgendes: Fördern Sie den Dialog mit Ihren Mitarbeitenden und schulen Sie sie hinsichtlich des richtigen Verhaltens bei einem Cybervorfall. Awareness-Maßnahmen spielen dabei eine entscheidende Rolle. Denn: So werden alle Mitarbeitenden an Bord des besagten Schiffes geholt. Alle Beteiligten sollten außerdem im Fall der Fälle wissen, wie und an wen sie einen potenziellen Vorfall zu melden haben. Durch die schnelle Reaktion der kontaktierten Expertinnen und Experten können Schäden frühzeitig abgewendet werden.

Das Klickverhalten im Detail: Welchen Einfluss haben Demografie, Branche und Uhrzeit?

Die Phishing-Simulation Phish-Test von SoSafe und Botfrei dient zur Erhebung der Grund-Awareness

Bei der jährlich stattfindenden Aktion „www.phish-test.de“ (Datensatz 3) – 2020 mit über 5.000 Teilnehmenden – erhebt SoSafe gemeinsam mit der Initiative Botfrei.de die Phishing Awareness unter Bürgerinnen und Bürgern. Dabei werden demografische Faktoren ermittelt, die bei der Analyse Berücksichtigung finden.

Die Ergebnisse liefern wenig Grund zur Beruhigung: Die durchschnittliche Awareness scheint eher niedrig zu sein. Etwa 31 % aller Teilnehmenden klickten auf mindestens eine der simulierten E-Mails, welche zur Erhebung versendet wurden.[31] Damit wäre knapp jeder dritte Social-Engineering-Angriff erfolgreich gewesen.

Interessant dabei: Die Auswertungen veranschaulichen nicht nur, wie schwer die Phishing-Maschen der Cyberkriminellen zu erkennen sind, sondern auch, dass unterschiedliche demografische Gruppen von Nutzenden auch unterschiedlich gut im Bereich Phishing-Awareness aufgestellt sind.

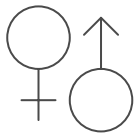
[31] Botfrei (2020). Phish-Test Ergebnisse: Männer klicken häufiger als Frauen.

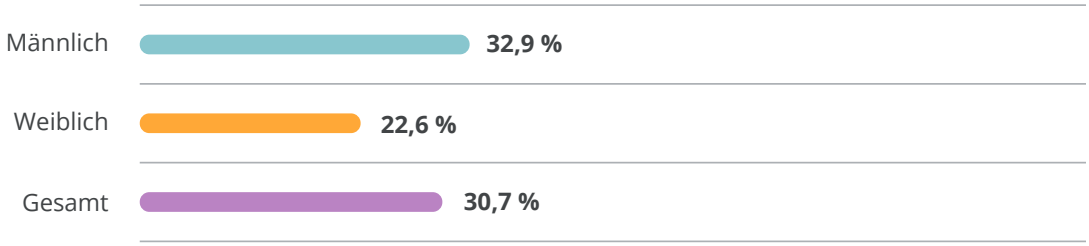
Phishing-Awareness nach demografischen Faktoren: der Mythos der sicheren „Digital Natives“

Männer klicken häufiger als Frauen

Fast jeder dritte männliche Teilnehmer (32,9 %) klickte auf mindestens eine der Phishing-Mails. Bei den Frauen waren es nur 22,6 %. Grundsätzlich war das Interesse von Männern am Thema Phishing aber deutlich höher als das der Frauen. Unter den Teilnehmenden der Erhebung befanden sich 78 % Männer und 22 % Frauen.

Klickraten nach Geschlecht

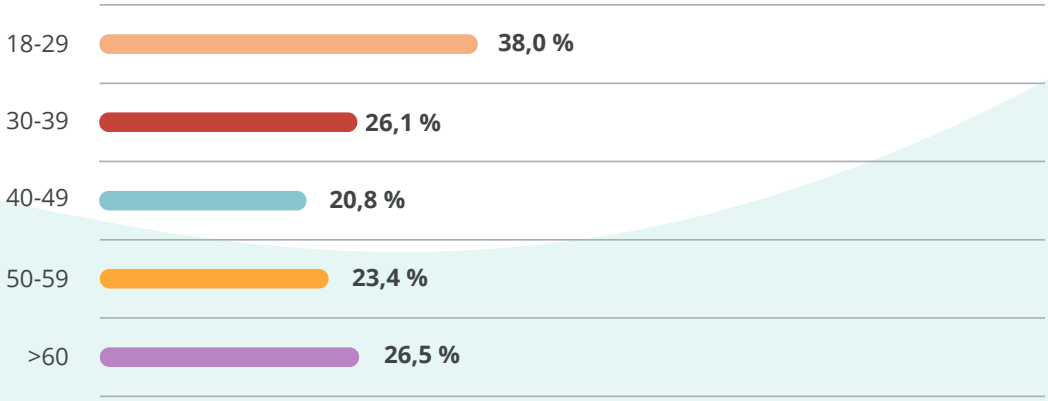




Jüngere klicken häufiger als Ältere

Die Vermutung, dass jüngere Nutzende oder „Digital Natives“ eine wesentlich höhere Medienkompetenz besitzen und somit auch in der Lage sind, Phishing-Mails zu erkennen, scheint naheliegend. Die Erhebung ergab aber genau das Gegenteil: Die anfälligste Altersgruppe bilden die 18- bis 29-Jährigen mit einer Klickrate von 38 %. Alle anderen Altersgruppen waren deutlich skeptischer beim Öffnen der E-Mails, im Durchschnitt klickten nur 25 %.

Klickraten nach Altersgruppe

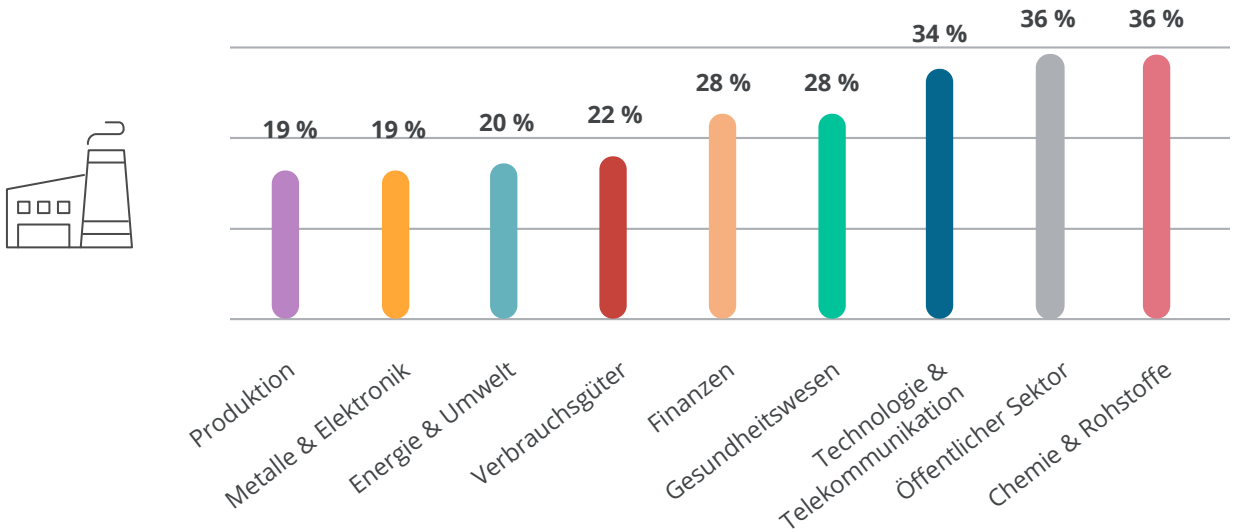


Neigen bestimmte Branchen zu höheren Klickraten?

Im Kontext der Simulationsdaten der SoSafe Awareness-Plattform (Datensatz 2) zeigen sich spannende Unterschiede zwischen verschiedenen Branchen. So scheinen insbesondere Organisationen aus dem öffentlichen Sektor, darunter etwa KRITIS-Organisationen wie Krankenhäuser, mit einer Klickrate von 36 % am anfälligsten für Phishing-Attacken (einen Erklärungsversuch liefert die Infobox auf S. 9). Auch in der Chemiebranche sowie in Technologie- und Telekommunikationsunternehmen klickt durchschnittlich mehr als jede und jeder dritte Mitarbeitende. Dahingegen beläuft sich die durchschnittliche Klickrate im produzierenden Gewerbe nur auf etwa 19 %. Ein Grund dafür könnte die verringerte Nutzung von Computerarbeitsplätzen beziehungsweise digitaler Kommunikationsmittel in diesem Bereich sein. Damit bliebe die Gefahr für Klicks auf Phishing-Mails allerdings dennoch hoch – denn so sind die Mitarbeitenden auch weniger geübt darin, Angriffe zu erkennen.

Insgesamt liegt mit einem Blick auf die Höhe der Klickraten die Vermutung nahe, dass IT-Sicherheit und insbesondere die Awareness der Mitarbeitenden in allen Bereichen der Wirtschaft noch nicht ausreichend priorisiert werden.

Klickraten nach Industrie[32]



[32] Datengrundlage: 1,4 Mio. simulierte Phishing-Angriffe aus der SoSafe Awareness-Plattform.

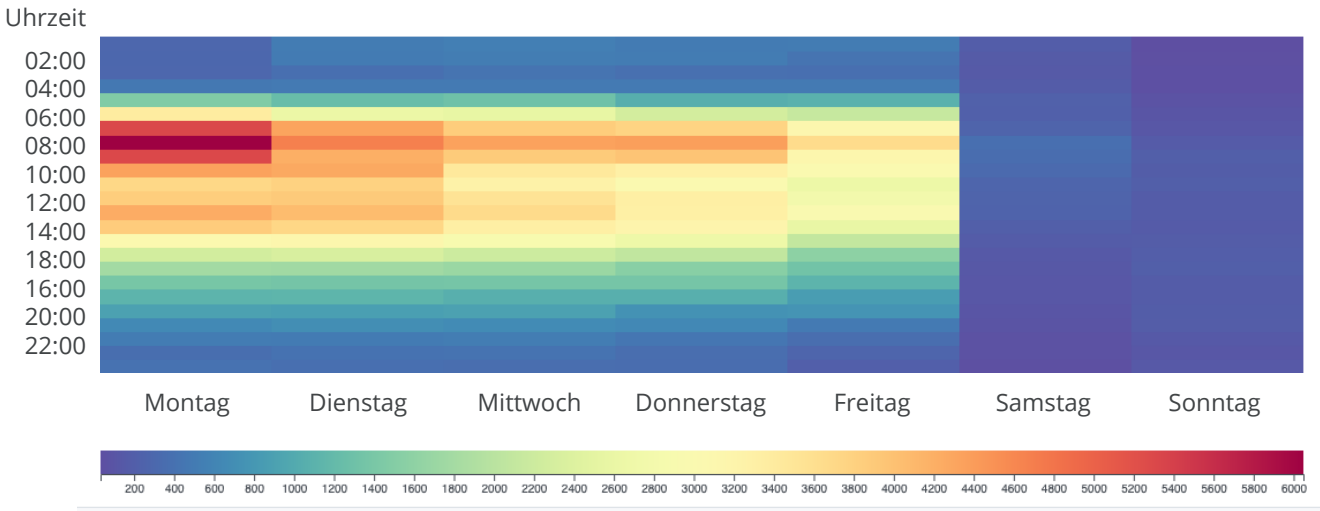
Der frühe Vogel klickt – das Angriffsrisiko im Zeitverlauf

Die Reaktionsdaten aus der SoSafe Phishing-Simulation (Datensatz 2) geben einen spannenden Einblick in den zeitlichen Verlauf des Angriffsrisikos an einem typischen Arbeitstag. Der erste Kaffee scheint dabei eine entscheidende Wirkung auf das Klickverhalten zu haben. So klicken vor allem montagmorgens vor acht Uhr viele Mitarbeitende auf Phishing-Mails. Auch über die restliche Woche hinweg scheint das Risiko für einen erfolgreichen Angriff besonders morgens hoch zu sein. Um die Mittagspause herum wird ebenfalls häufiger geklickt als im restlichen Verlauf des Nachmittags. Unabhängig davon scheint das Risiko zu Beginn der Woche höher als zu deren Ende zu sein. Es scheint also, dass Angestellte in Organisationen zu den genannten Zeitpunkten in der Tat unvorsichtiger im Umgang mit Cybergefahren sind.

Mitarbeitende klicken häufiger morgens als nachmittags und verstärkt zu Beginn der Woche.

Zum einen könnte dies daher rühren, dass morgens und mittags oftmals eine erneute Flut an Mails im Postfach darauf wartet, geöffnet zu werden und Mitarbeitende sich schnell über To-Do's und Neuigkeiten einen Überblick verschaffen möchten. Potenzielle Phishing-Mails gehen in der Masse dann schneller unter. Zum anderen könnten Mitarbeitende zu diesen Uhrzeiten weniger wachsam sein, weil sie noch nicht in ihren eigentlichen Workflow eingetaucht sind oder gedanklich noch oder bereits bei anderen Themen sind. Ein Ansatz für die Sensibilisierung kann und sollte also sein, Mitarbeitende auch dabei zu unterstützen, ihre Mail-Bearbeitung so zu gestalten, dass das Risiko für unbedachtes Klicken verringert wird.

Klicks auf Phishing-Mails in einer durchschnittlichen Woche[33]



[33] Datengrundlage: 1,4 Mio. simulierte Phishing-Angriffe aus der SoSafe Awareness-Plattform.

DEKRA DIGITAL

innovating safety

Herausforderung Homeoffice – IT-Sicherheit in Zeiten zunehmender Digitalisierung

Ein Interview mit Dr. Kerim Galal, Managing Director bei DEKRA DIGITAL

Dr. Kerim Galal ist Managing Director bei DEKRA DIGITAL sowie Executive Vice President Innovation & Digitalization bei DEKRA – und für die Zukunftsthemen Strategie, Innovation und Digitalisierung verantwortlich. Gemeinsam mit Partnern und Start-ups arbeitet DEKRA DIGITAL an Technologien wie IoT, Cyber Security oder Künstlicher Intelligenz. Vor seiner Tätigkeit bei DEKRA war er bei McKinsey & Company tätig und hat an der EBS in Oestrich-Winkel promoviert.

Inwiefern hat das letzte Jahr Veränderungen im Bereich der Digitalisierung, z. B. in der Art des Zusammenarbeitens, gebracht?

Die Corona-Pandemie hat das Zusammenarbeiten in einer bis dahin unbekannten Geschwindigkeit grundlegend verändert – vor allem durch Remote Work. Das war auch für uns bei DEKRA DIGITAL eine Umstellung. Durch eine gute IT-Infrastruktur und die bereits jahrelange Arbeit mit Kollaborationsplattformen wie Slack und Teams haben wir uns aber schnell adaptiert.

Das ständige Arbeiten im Homeoffice hat auch viele andere Unternehmen vor große Herausforderungen bei der Digitalisierung gestellt, insbesondere im Bereich IT-Sicherheit. Gerade zu Hause ist beispielsweise die Versuchung groß, Firmensysteme und privat genutzte Lösungen zu vermischen. Sich außerhalb der gesicherten IT-Infrastruktur des Unternehmens zu bewegen, birgt aber gerade für die IT-Sicherheit große Gefahren.

Welchen Zusammenhang sehen Sie zwischen Digitalisierung und Cyber Security?

Alle Lebensbereiche werden zunehmend digitalisiert. Ob wir ins Büro fahren, einen Voice Assistant nutzen oder unseren Laptop aufklappen – Daten, und die damit einhergehenden Risiken, sind omnipräsent. Diese Vernetzung bietet viele Vorteile, aber auch Angriffsfläche für Hacker mit klaren Auswirkungen auf die Cyber Security von Unternehmen und Einzelpersonen.

Unser Unternehmen steht seit knapp 100 Jahren für Sicherheit und hat sich zum Ziel gesetzt, Menschen auf der Arbeit, im Verkehr und zu Hause zu schützen – das möchten wir auch auf die digitale Sphäre übertragen. Im „Cyber Security Hub" vereint DEKRA DIGITAL deshalb Experten zu diesem Thema. Wir bündeln Expertise aus verschiedenen Bereichen, um Sicherheit in einer zunehmend digitalisierten Welt weiter zu gewährleisten – dazu gehört auch IT-Sicherheit.

DEKRA ist führend sowohl im Bereich der Sicherheitszertifizierung als auch bei der Schulung von Mitarbeitenden – welche Herausforderungen sehen Sie für das kommende Jahr an der Schnittstelle von Sicherheit und Faktor Mensch?

Auch im kommenden Jahr wird das neue Homeoffice-Setting an dieser Schnittstelle eine entscheidende Rolle spielen: Für Beschäftigte ist das Einhalten von gewissen Mindeststandards der IT-Sicherheit essenziell, um sich selbst und das Unternehmen zu schützen.

Schon der heimische Arbeitsplatz kann sich als problematisch erweisen. Der Couchtisch, an dem der Rest der Familie spielt oder fernsieht, lässt nicht nur die Grundanforderungen an die Ergonomie vermissen, sondern auch die an die IT-Sicherheit.

Gerade in der aktuellen Situation sollten Unternehmen deshalb nicht nur Richtlinien definieren und technische Sicherungsmaßnahmen einleiten, sondern ihre Mitarbeiter für die zunehmenden Cyber-Risiken sensibilisieren – Stichwort „Social Engineering" – und entsprechende IT- Sicherheitstrainings auffrischen.

Social-Engineering-Trends 2021: Cyberkriminelle rüsten weiter hoch

2020 war geprägt vom Ausbruch der Pandemie und einer eindeutigen Verschärfung der Bedrohungslage – vor allem in Bezug auf den Faktor Mensch. Es war ein schwieriges Jahr für Organisationen und Sicherheitsverantwortliche – aber ein erfolgreiches Jahr für Angreifende und Ransomware-Gruppen. Leider gibt es keinen Grund zur Entspannung: Zukünftig ist sowohl mit einer Steigerung des Angriffsaufkommens als auch mit neuartigen Angriffen zu rechnen. Denn: Innovationen sind mittlerweile fester Teil einer hochgradig professionalisierten Hacker-Industrie geworden.

Auf welche Cyber-Angriffstaktiken und -methoden müssen sich Organisationen also 2021 gefasst machen? Unsere Expertinnen und Experten, Kundinnen und Kunden und Partnerorganisationen sehen die folgenden Trends:

Neues Arbeiten – neue Kanäle

Durch den Wechsel ins Homeoffice kamen Kollaborationstools wie Teams und Zoom in vielen Organisationen verstärkt zum Einsatz. Laut Bitkom werden in Deutschland auch künftig mehr Mitarbeitende dauerhaft im Homeoffice arbeiten als noch vor der Pandemie – voraussichtlich über 10 Millionen.[34] Für Angreifende sind dafür genutzte Kollaborationstools ein attraktiver Weg in die Systeme von Unternehmen. Zahlreiche Phishing-Kampagnen versuchten 2020 beispielsweise, Zugangsdaten zu den entsprechenden Tools über Einladungs-E-Mails und nachgeschaltete Login-Masken zu erbeuten. Das Problem: Viele Mitarbeitende sind noch unvertraut mit den Cloud-Lösungen und fühlen sich relativ sicher innerhalb dieser Kanäle – firmeninterne Cloud-Chat-Tools werden als geschützter Raum wahrgenommen.

So ist es wenig überraschend, dass Credential-Theft-Angriffe, die auf das Erlangen von Zugangsdaten für diese Tools zielen, stark zugenommen haben. Da die Bedeutung dieser Tools auch weiterhin zunehmen wird, muss auch weiterhin mit einem Anstieg derartiger Angriffe gerechnet werden.

Doppel-Erpressungen nehmen zu

Eine neue Ransomware-Generation war bereits im letzten Jahr zu beobachten und wird auch die zukünftige Gefahrenlage maßgeblich prägen. Die Ransomware-Gruppen tragen Namen wie „Sodinokibi“ oder „Egregor“ und gehen nach dem „Double Extortion“-Prinzip („Doppel-Erpressung“) vor: Wird Lösegeld nicht gezahlt, werden Daten sogar veröffentlicht – mit kostspieligen Folgen für die Opfer.

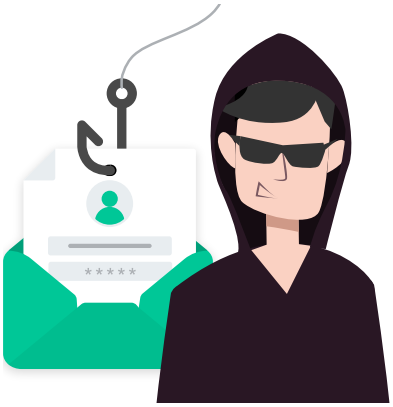
Klassische Incident-Response-Strategien und Back-ups reichen also nicht mehr aus, um sich vor Lösegeldzahlungen zu schützen. Die Egregor-Gruppe wurde etwa im September 2020 erstmals aktiv und hat bereits jetzt namhafte Opfer wie Barnes & Noble, Ubisoft, Crytek und Randstad. Die Angreifenden zünden eine neue Eskalationsstufe und stärken so gleichzeitig ihre Verhandlungsposition. Deshalb ist zu erwarten, dass weitere Gruppen schon bald auf das Prinzip aufspringen werden. Umso wichtiger wird damit auch das Thema Prävention.

[34] Bitkom (2020). Mehr als 10 Millionen arbeiten ausschließlich im Homeoffice.

KI-gestütztes Social Engineering wird verbreiteter

Bereits 2019 wurde auf dem BSI-Sicherheitskongress vor der Möglichkeit eines KI-gestützten „Voice-Phishing-Bots zur Vorlegitimierung einer schadhaften E-Mail"[35] gewarnt. Dabei wurde ein theoretischer Angriff geschildert, der auf Basis künstlicher Intelligenz (KI) die Stimme eines Vorgesetzten imitieren könnte. Nur wenige Monate später wurde der erste echte Fall bekannt. Ein Mitarbeiter eines britischen Energieversorgers wurde vom vermeintlichen CEO des deutschen Mutterkonzerns angerufen und aufgefordert, Geld auf ein ungarisches Bankkonto zu überweisen. Der oder die Kriminelle stahl 220.000 Euro.

Es ist davon auszugehen, dass dieser Anruf mithilfe des beschriebenen trainierten KI-Modells umgesetzt wurde. Während derartige Angriffe noch die Ausnahme sind, wird der anteilige Einsatz von KI im Bereich Social Engineering weiter zunehmen, zum Beispiel auch zur Generierung von schriftlichem Text. Der Grund: Die Modelle lassen sich immer einfacher trainieren, und erfolgreiche Fälle steigern die Akzeptanz der neuen Technologie bei den Hackern.



„Phishing is here to stay"

Klassische Taktiken, wie Phishing und Business-Email-Compromise, werden allerdings auch weiter das Kerngeschäft der Cyberkriminellen bleiben. Und durch die neue Arbeitsrealität vieler Mitarbeitenden werden diese Taktiken noch attraktiver. Denn: Die Absichten und das Risiko potenziell schädlicher Mails lassen sich im Remote-Setting schlechter überprüfen.

Der Flurfunk schützt, das ergab auch eine SoSafe Analyse (siehe S. 24): Beim dezentralen Arbeiten ist die Klickrate auf simulierte Angriffe dreimal so hoch wie bei Mitarbeitenden im Büro. Verdächtige Nachrichten lassen sich schwerer validieren, wenn der Austausch nur auf notwendige Meetings oder Chatnachrichten reduziert ist. Das wird den Hackern auch zukünftig in die Hände spielen und das Angriffsaufkommen auf einem weiterhin sehr hohen Niveau belassen.

[35] Hellemann, Niklas (2021). Das Spiel mit der Angst - Erfolgsfaktoren neuartiger Social-Engineering-Angriffe im Kontext der COVID-19-Pandemie. Kongressband des 17. Deutschen Sicherheitskongresses des BSI.

Fazit & Empfehlungen: Wie minimieren Organisationen ihr Human Risk?

Die Auswertungen in diesem Report veranschaulichen: Mensch und IT-Sicherheit sind eng miteinander verknüpft. Diese Einsicht ist gerade in einer Zeit, die von allgemeiner Unsicherheit und einer verschärften Cyber-Bedrohungslage geprägt ist, von großer Bedeutung. Denn wenn sich aktuelle Angriffstaktiken immer häufiger auf die Manipulation menschlicher Emotionen konzentrieren und technische Sicherheitsvorkehrungen allein nicht mehr ausreichen, liegt es an Organisationen, ihre „menschliche Firewall" nachhaltig zu stabilisieren. Mitarbeitende müssen also aktiv in die Stärkung der IT-Sicherheit eingebunden werden.

Wie können Organisationen dem wachsenden Human Risk aber nun ganz konkret begegnen und Mitarbeitende im Cyber-Security-Bereich von Risiko- zu Sicherheitsfaktoren machen?

Cyberresilienz aufbauen

Stellen Sie Ihren Mitarbeitenden Ressourcen zur Verfügung, die ein Bewusstsein für die Gefahren und damit eine unternehmensweite Cyber-Resilienzkultur fördern. Durch vielfältige Schulungsmaßnahmen geben Sie Ihren Mitarbeitenden die Möglichkeit, sich im Bereich Cyber Security zu befähigen. Alle Mitarbeitenden – nicht nur IT-Spezialisten müssen als Bestandteil einer geschlossenen Verteidigungslinie gegen Cyberangriffe gedacht werden.

Awareness ganzheitlich gestalten

Nur durch eine Kombination aus vielfältigen Schulungsmaßnahmen lässt sich eine echte Handlungskompetenz bei Ihren Mitarbeitenden aufbauen. Basierend auf lernpsychologischen Erkenntnissen, bildet die Kombination aus Phishing-Simulation, Nano-Lerneinheiten und Storytelling einen nachhaltigen und wirksamen Lernkontext, der im Sinne Ihrer Mitarbeitenden gestaltet ist.

Flexibel und kontinuierlich schulen

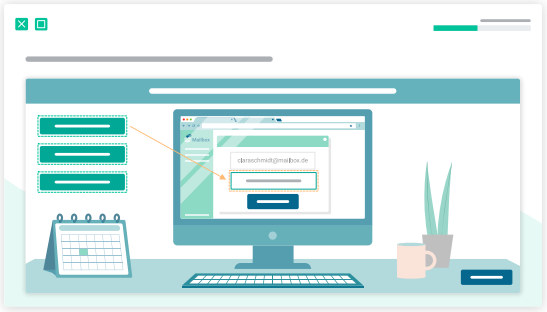
Cyberkriminelle sind – wie das Jahr 2020 noch einmal eindrücklich gezeigt hat – schnell in der Umsetzung neuer Ransomware, die sich immer am aktuellen Zeitgeschehen orientiert. Auch die Awareness-Maßnahmen müssen sich flexibel daran anpassen und auf neue Taktiken unmittelbar reagieren. Der schnelle Wandel der Cyberkriminalität zeigt auch: Punktuelle Lerneinheiten sind nur kurzfristig wirkungsvoll, daher ist kontinuierliches Schulen essenziell.

DSGVO-konforme Anbieter wählen

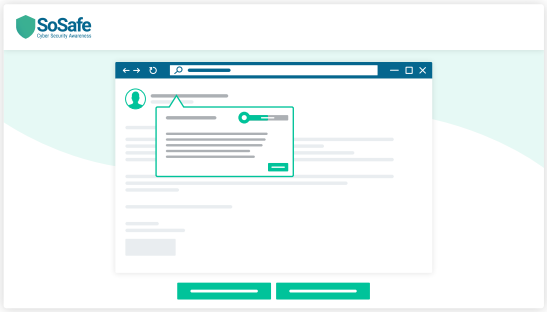
Schaffen Sie in Ihrem Unternehmen absolute Rechtssicherheit und entscheiden Sie sich für EU-Anbieter mit Datenverarbeitung auf EU-Servern. Nur so können Sie den Schutz der sensiblen Daten Ihrer Mitarbeitenden 100 % DSGVO-konform gewährleisten und Datensicherheit garantieren.

Über SoSafe

Die SoSafe GmbH mit Sitz in Köln ist Anbieter einer interaktiven Schulungsplattform zur IT-Sicherheit und einer der Marktführer im Bereich Awareness-Building in der DACH-Region. Das rund 100-köpfige Team besteht aus Expertinnen und Experten aus verschiedensten Fachbereichen: Von IT-Sicherheit über Psychologie und Pädagogik bis hin zu Kommunikationsdesign. Über ein modernes und modulares E-Learning sowie kontinuierliche Phishing-Simulationen sensibilisiert und schult die Awareness-Plattform von SoSafe Mitarbeitende im Umgang mit allen Arten von Cybergefahren. Das Training verläuft interaktiv, motivierend und zu 100 % datenschutzkonform und trifft so auf höchste Akzeptanz bei Personalvertretungen und Mitarbeitenden.

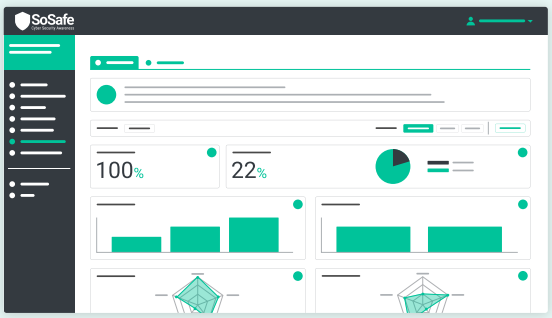


Modulares E-Learning

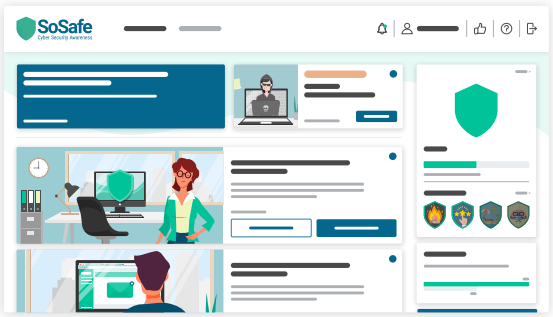


Kontinuierliche Phishing-Simulation

Mit verständlichen KPIs und einem differenzierten Reporting wird sowohl das Human Risk als auch der Erfolg der Cyber-Security-Schulungsmaßnahmen endlich messbar und sichtbar. Zahlreiche europäische Organisationen verschiedenster Branchen vertrauen auf den Schulungseffekt der SoSafe Awareness-Plattform, darunter etwa Aldi und Vattenfall, zahlreiche Stadtwerke sowie Landesverwaltungen, namhafte Kliniken und Universitäten wie die RWTH Aachen.



Differenziertes Reporting



E-Learning Plattform

Branding Engine

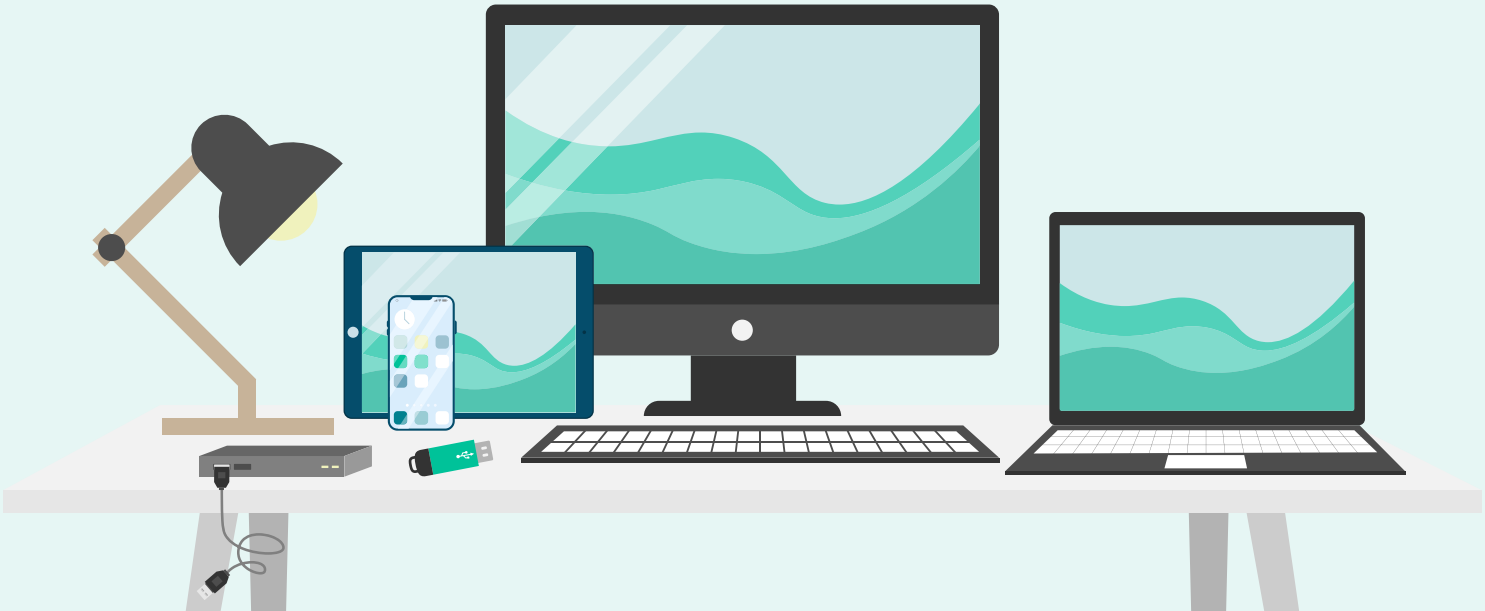
Die SoSafe Awareness-Plattform ist rund um den Menschen und seine Bedürfnisse entworfen, um allen Mitarbeitenden einen bewussten Umgang mit IT-Sicherheit zu ermöglichen. SoSafe's Lerneinheiten sind unterhaltsam und leicht zugänglich – die Auswertungen anonym, sodass personenbezogene Daten jederzeit geschützt sind. Das Training basiert auf aktuellen lern- und verhaltenspsychologischen Erkenntnissen: Die Awareness-Plattform setzt auf interaktive und multimediale Methoden, die kontinuierlich statt punktuell sensibilisieren. Darüber hinaus können E-Learning und Phishing-Simulation über die Customization Engine inhaltlich und optisch auf interne Richtlinien, branchenspezifische Bedürfnisse sowie Corporate Identity abgestimmt werden.

Kurze, aber präzise Micromodule schaffen zeiteffizient ein erhöhtes Sicherheitsbewusstsein bei den Mitarbeitenden. Zugängliche Charaktere begleiten sie auf individuellen Lernpfaden durch die Plattform mit ihren realitätsnah gestalteten Inhalten.

Gamification-Elemente, wie Abzeichen und Level, motivieren zusätzlich zur fortwährenden Auseinandersetzung mit dem komplexen Thema IT-Sicherheit. Über ein Reporting-Dashboard ermöglicht SoSafe Entscheiderinnen und Entscheidern außerdem die differenzierte und anonymisierte Auswertung der Erfolge. Technische und psychologische KPIs geben Organisationen Aufschluss darüber, wie hoch ihr Human Risk ist, wie effektiv die Awareness-Maßnahmen sind und somit auch wie Mitarbeitende noch passgenauer sensibilisiert werden können.

Die SoSafe Plattform ist ein cloudbasierter Service und muss nicht in ein bestehendes System integriert werden. Ein eigenständiges Cloud LMS (Learning Management System) gestattet es, sofort und ohne Implementierung zu starten. Für Unternehmen mit eigenem LMS bietet SoSafe als einziger Anbieter durch das sogenannte SCORM Streaming stets aktualisierte und angepasste Inhalte.

SoSafe wird in Deutschland entwickelt und läuft ausschließlich auf deutschen Servern. Daten werden vollständig DSGVO-konform gespeichert und verarbeitet. Das spezielle Compliance-Dashboard erlaubt es Organisationen zudem, den Status der Sensibilisierung im Rahmen bestehender Compliance Frameworks (z.B. ISO-27001) auszugeben und so einen entsprechenden Nachweis zeitsparend zu erbringen.



Autoren

Dr. Niklas Hellemann, SoSafe GmbH
Ann-Kathrin Krane, SoSafe GmbH
Friederike Kneip, SoSafe GmbH

Interviewpartner

Bert Skaletski, Chief Information Security Officer, Merck KGaA

Prof. Dr. Michael Meier, Lehrstuhl für IT-Sicherheit an der Universität Bonn, Head of Cyber Security am Fraunhofer FKIE

Dr. Kerim Galal, Managing Director bei DEKRA DIGITAL, Executive Vice President Innovation & Digitalization bei DEKRA

Layout & Design

Clara Wördenweber, SoSafe GmbH
Annalena Eckertz, SoSafe GmbH

Kontakt

E-Mail: info@sosafe.de
Telefon: +49 221 6508 3800

Weitere Informationen

www.sosafe.de

Digitale Version des Human Risk Review 2021:
www.sosafe.de/human-risk-review-2021

SoSafe
Cyber Security Awareness

SoSafe GmbH
Ehrenfeldgürtel 76, 50823 Köln
www.sosafe.de | info@sosafe.de